it-safe.at

it-safe: Achten Sie gerade jetzt auf Cybersicherheit!

Social Engineering - der Mitarbeiter als Angriffsziel

Tipps zur Sensibilisierung und zur Abwehr von Spionage am Arbeitsplatz

Stand: 15.03.2017

Unternehmen investieren viel Geld in technische Zugangsbarrieren, um ihre IT vor Angriffen von außen zu schützen und den unerlaubten Datenzugriff von extern zu unterbinden. Für Hacker wird es somit immer aufwändiger, diese technischen Schranken zu umgehen oder zu durchbrechen. Daher verlegen sich viele Kriminelle auf eine einfachere Methode, um an vertrauliche Informationen von Unternehmen zu kommen: Social Engineering.

Social Engineers nutzen menschliche Verhaltensweisen wie Hilfsbereitschaft, Bequemlichkeit oder Gehorsam aus, um an geheime Informationen oder unbezahlte Dienstleistungen zu kommen. Zu diesem Zweck spionieren sie zuerst oft das persönliche Umfeld ihres Opfers aus und täuschen falsche Tatsachen oder Identitäten vor.

Ziel der Aktion ist es, die Person durch zwischenmenschliches Interaktion zu beeinflussen und ein bestimmtes Verhalten zu erreichen. Das kann zum Beispiel die Preisgabe von vertraulichen Informationen sein, aber auch der Kauf eines Produktes oder die Freigabe von Finanzmitteln.

Diese Vorgangsweise kann auch zum Ziel haben, Zugang in ein fremdes Computersystem zu bekommen, um dort vertrauliche Daten einzusehen. Man spricht dann auch von **Social Hacking**.

Vorgehensweise bei Social Engineering

Schritt 1:

Zuerst sammeln die Angreifer (persönliche) Informationen über die Zielperson und das Unternehmen

Das passiert etwa mithilfe von Pishing-Mails („Sie haben gewonnen", „Ich möchte dich kennenlernen" etc.) oder zielgerichtet direkt auf der Firmenwebsite, wo oft Namen und Kontaktdaten des Managements zu finden sind. In sozialen Medien wie Facebook, LinkedIn, Xing usw. kommen manchmal gefälschte Profile zum Einsatz.

Schritt 2:

In einem zweiten Schritt erfolgt die persönliche Kontaktaufnahme

Die gesammelten Informationen helfen dabei, möglichst glaubwürdig zu wirken. Oft werden verschiedene Mitarbeiter desselben Unternehmens ausgefragt und die herausgefundenen Details kombiniert und für weitere Kontaktaufnahmen benutzt. Sehr oft sind die Angreifer auch psychologisch gut geschult und überrumpeln ihre Opfer regelrecht am Telefon. Dabei werden zum Beispiel folgende Methoden eingesetzt:

- Es wird Insiderwissen vorgetäuscht.
- Eine Menge an Fachvokabular wird bewusst verwendet.
- Es wird an eine dritte Person – meist eine höhere Stelle – als Rechtfertigung für den Anruf verwiesen.
- Sehr oft geben sich Angreifer als „wichtige Person" aus, z.B. ein Support-Mitarbeiter, ein Bekannter vom Chef, ein Journalist, der dringend Informationen benötigt usw.
- Es wird aus „besonderen Gründen" um einen Gefallen gebeten.
- Es wird Zeitdruck ausgeübt. Alles muss sehr rasch gehen.
- Sollte das Opfer Widerstand leisten, wird auf die Konsequenzen hingewiesen, bis hin zur Drohung.

Schritt 3:

Angriffszweck: Passwort knacken

Meist fokussieren sich Angreifer auf den wichtigsten Teil Ihres Sicherheitssystems: das Passwort. Denn damit können die meisten technischen Zugriffsbarrieren und Überwachungssysteme umgangen werden. Haben die Angreifer einmal Zugang zum Unternehmens-Netzwerk, werden dort vertrauliche Unternehmensinformationen abgesaugt: Kundendatenbanken, Verträge und Patente usw.

Einzige Abhilfe:
Jeder einzelne Mitarbeiter verwendet sein eigenes, sicheres Passwort und teilt dieses unter keinen Umständen mit anderen. Jeder neue Mitarbeiter (auch Aushilfen für wenige Stunden!) erhält einen eigenen Zugang.

Dieses Passwort darf niemals herausgegeben werden – weder unter Druck eines telefonischen Vorwands (z.B. eines „Supportanrufs") noch schriftlich, womöglich mittels Sticker am Monitor oder unterm Keyboard. Dies hebelt nicht selten die komplette IT-Sicherheit aus!

Abwehr von Social Engineering

Klären Sie Ihre Mitarbeiter über das Risiko von Social Engineering auf! Motivieren Sie Ihre Mitarbeiter, in Sicherheitsbelangen auf Ihr „Bauchgefühl" zu achten und einfach rückzufragen, wenn ihnen eine Situation komisch oder verdächtig vorkommt.

Definieren Sie, was alles vertraulich ist, und auch wo keinesfalls über vertrauliche Dinge gesprochen werden sollte. Ein belanglosens Plaudern im Kaffee an der Ecke kann schnell durch einfaches Mitlauschen durch Dritte zum Risiko werden.

Tipps zu Social Engineering Abwehr

- Kennen Sie den Absender einer E-Mail nicht, sollten sie stets misstrauisch sein.
- Bei Anrufen sollten auch scheinbar unwichtige Daten („Der Kollege ist im Urlaub") nicht sorglos an Unbekannte weitergegeben werden. Sie können diese Informationen für weitere Angriffe nutzen.
- Geben Sie keine Mobiltelefonnummer oder Durchwahl von Vorgesetzten oder Mitarbeiter/innen an unbekannte Personen weiter. Bieten Sie stattdessen an, dass zurückgerufen wird.
- Bei Antworten auf eine E-Mail-Anfrage sollten unter keinen Umständen persönliche oder zahlungsrelevante Daten preisgegeben werden, egal von wem die Nachricht zu kommen scheint.
- Klicken Sie nicht auf Links aus E-Mails, die die Eingabe persönlicher Daten verlangen. Geben Sie stattdessen die URL selbst im Browser ein. So vermeiden Sie gefälschte Websites.
- Bei Unklarheit über die Echtheit des Absenders oder die Authentizität der E-Mail, fragen Sie telefonisch nach. Die Rückrufnummer sollte aus einer unabhängigen Quelle stammen (Telefonbuch) und nicht aus dem vorangegangenen E-Mail oder Anruf.
- Sperren Sie konsequent den Bildschirm beim Verlassen des Arbeitsplatzes damit Betriebsfremde, die sich Zutritt zum Gebäude erschlichen haben, keinen Zugriff auf das Firmennetzwerk haben.
- Konsequentes Abräumen der Schreibtische am Ende des Arbeitstags
- Zugangspassworte werden nur dann zurückgesetzt, wenn der unmittelbare Vorgesetzte dies anordnet oder der Mitarbeiter persönlich beim Helpdesk vorspricht.
- Alle Mitarbeiter tragen deutlich sichtbar ihre Firmenausweise, Fremde sind leicht zu erkennen
- Alle Mitarbeiter nutzen ihre elektronischen Zugangskarten.
- Alle Besucher werden beim Empfang abgeholt und sind nie unbeaufsichtigt im Gebäude oder auf dem Firmengelände.