TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Social Engineering Kampagne

Um die Informationswerte eines Unternehmens angemessen zu schützen, müssen sich die Verantwortlichen bewusst sein, über welche Wege unternehmensinterne Informationen verloren gehen bzw. verfälscht werden können. Zieht man diesbezüglich alle möglichen Faktoren in Betracht, so wird schnell deutlich, dass menschliches Fehlverhalten oft die Ursache ist und die größten Schwachstellen im Unternehmen sich somit nicht zwingend in der Technik befinden. Über Manipulation von Mitarbeitern versuchen Angreifer, sich Zutritt zu Räumlichkeiten, Zugang zu Systemen und Zugriff auf Daten zu verschaffen, um unternehmens- bzw. kundenkritische Informationen zu manipulieren oder zu stehlen.

(Social-) Hacker gehen dabei sehr vielfältig vor: Sie nutzen die Gutgläubigkeit, Unwissenheit, Bequemlichkeit und das Vertrauen der Angestellten aus und machen sie so unbewusst zu ihren Helfern. Doch das muss nicht sein! Neben angemessenen technischen Sicherheitsmaßnahmen und Notfallplänen erfordert ein wirkungsvolles IT-Sicherheitskonzept eine Sensibilisierung der Mitarbeiter für das Thema Informationssicherheit.

Mit einer individuell auf Ihr Unternehmen zugeschnittenen Social Engineering Kampagne unterstützen wir Sie, Erkenntnisse über das aktuelle Sicherheitsniveau in Ihrem Unternehmen zu erlangen. Die Ergebnisse können als Basis für adäquate Security Awareness Maßnahmen dienen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter nachhaltig zu stärken.

Vorgehensweise

Unsere Experten agieren nach Absprache mit Ihnen wie „richtige“ Angreifer und versuchen ohne Zugangsdaten oder Insiderwissen an Informationen in Ihrem Unternehmen zu gelangen. Zur Planung und Durchführung von Social Engineering Kampagnen wenden wir die Methodik des „Social Engineering Attack Cycle“ an:

I. Recherche und Vorbereitung

Zunächst werden so viele Informationen wie möglich über Ihr Unternehmen gesammelt. Je mehr Insiderinformationen vorliegen, desto leichter fällt es, eine Vertrauensbeziehung aufzubauen.

II. Pretexting (Schaffen einer Beziehung)

Für jeden Angriff wird eine Geschichte bzw. ein Vorwand erarbeitet, die den Angriff entweder als unauffällige oder übliche Handlung tarnt, oder von dem Angriff als solchem ablenkt. Das primäre Ziel ist das Schaffen einer Vertrauensstellung gegenüber einem Mitarbeiter.

III. Exploit (Ausnutzen der Beziehung)

Die vorher erlangte Vertrauensstellung wird eingesetzt, um den Angriff durchzuführen. In dieser Phase wird versucht, den gewünschten Zutritt, Zugang oder Zugriff zu erlangen.

IV. Sammeln, Analysieren und Bewerten

Besteht Zutritt, Zugang oder Zugriff auf Informationen in Ihrem Unternehmen, werden davon so viele wie möglich gesammelt. Diese können entweder noch während des Angriffs analysiert werden, um daraus Möglichkeiten weiterer Angriffe abzuleiten, oder im Nachhinein untersucht und bewertet werden.

Mit dieser Methodik können unterschiedliche Arten von

Cyber Security

Angriffen durchgeführt werden, dir wir individuell für Sie zusammenstellen (Auszug):

- Phishing: Versuch, über gefälschte E-Mails an sensible Daten eines Nutzers zu gelangen, um diese für einen Angriff zu nutzen.
- Vishing: Versuch, über Telefonate (Voice Phishing) die Benutzer dazu zu verleiten, vertrauliche Informationen bekannt zu geben.
- Zutritt durch Überzeugung: Versuch, Zutritt zu relevanten Räumen und nach Möglichkeit dort Zugriff auf interne IT und Netzwerke zu erlangen.
- Tailgating/Piggybacking: Versuch, sich Zutritt in gesicherte Bereiche zu verschaffen, indem sich der Angreifer Mitarbeitern physikalisch einfach anschließt (z.B. Tür aufhalten).
- Alternative Zugangswege: Untersuchung des Standorts auf mögliche alternative Zugangswege zu internen Netzwerken (z.B. über WLAN, mobile Geräte etc.).
- Baiting: Streuung von Köderobjekten als Trojanische Pferde vor Ort oder per Post. Üblicherweise handelt es sich hierbei um präparierte USB-Sticks.

Alle genannten Methoden und später auch real durchgeführten Angriffe erfolgen so, dass durch die Ausführung kein realer Schaden entsteht.

Ihr Nutzen

- Aktueller Status der Unternehmenssicherheit sowie des Sicherheitsbewusstseins der Mitarbeiter
- Managementbericht, in dem die durchgeführten Angriffe, ein Lagebericht zum Sicherheitsniveau sowie ein Maßnahmenkatalog mit Empfehlungen zur Beseitigung der Schwachstellen aufgeführt sind
- Grundlage für Security Awareness Maßnahmen als Bewusstseinsentwicklung und Wirksamkeitsmessung in Bezug auf den vertraulichen Umgang mit Unternehmensinformationen
- Durch das tatsächliche Eintreten von vorher theoretisch dargestellten Bedrohungen erfolgt eine emotionale Verankerung des Erlernten und Erlebten
- Die regelmäßige Kombination von beauftragtem Social Engineering und Security Awareness Kampagnen eignet sich, um Ihr Unternehmen vor Angriffen nachhaltig zu schützen

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com