CYBERSEC-NG
Swiss Cybersecurity

Physical Social Engineering

Unter dem Begriff Social Engineering versteht sich generell die gezielte Manipulation von Menschen, mit dem Ziel, Zugriff auf Computersysteme oder Gebäude zu erlangen. Beim physischen Social Engineering versucht einer unserer Social Engineering Experten Zutritt zu einem Gebäude zu erlangen. In diesem Zusammenhang wird häufig sogenanntes Tailgating (Durchschlüpfen) eingesetzt. Der Angreifer wartet hierbei, bis eine berechtigte Person eine Tür öffnet und schleicht hinterher. Ziel eines physischen Social Engineerings ist, die Effektivität der implementierten physischen Sicherheitsmassnahmen (Sicherheitspersonal, Zutrittssysteme, etc.) und das Verhalten der Mitarbeiter zu analysieren und Risiken festzustellen.

ÜBERPRÜFBARE SICHERHEIT

In der Theorie funktionieren die implementierten physischen Sicherheitsmassnahmen und Policies meistens gut. Es fragt sich jedoch, ob die Massnahmen auch im Ernstfall, also der Praxis richtig angewendet werden. Mit unserem physischen Social Engineering können Sie Ihr Personal durch einmalige oder wiederholte Angriffe schulen, Sicherheitsschwachstellen feststellen und proaktiv Gegenmassnahmen einleiten. So sind Sie und Ihr Personal für den Ernstfall vorbereitet.

AWARENESS

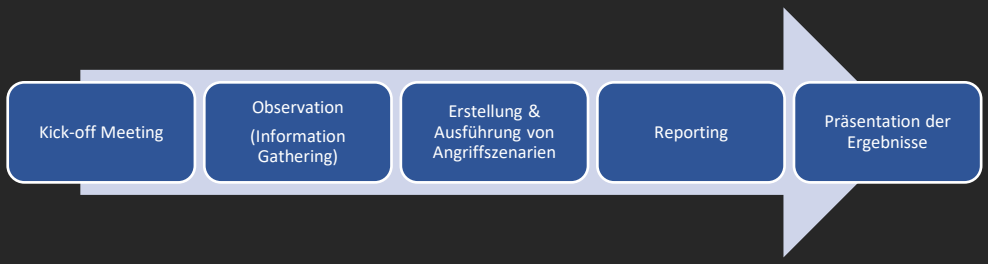
Damit die physische Sicherheit angemessen umgesetzt wird, muss das Personal geschult und sich den Sicherheitsrisiken bewusst sein. Wann immer möglich liefern wir audiovisuelle Aufzeichnungen der Gespräche zwischen unserem Social Engineer und Ihren Mitarbeitenden, die wertvoll für weiterführende Awareness Schulungen sind.

RISK MANAGEMENT

Damit angemessen mit Risiken umgegangen werden kann, müssen diese bekannt sein.
Durch unser physisches Social Engineering Audit werden Risiken sichtbar und Sie erhalten einen Überblick über die Schwachstellen in Ihrer physischen Sicherheit (inkl. Risikobewertung).

Vorgehensweise

Wir lehnen uns bei der Durchführung von Social Engineering Audits an den Penetration Testing Execution Standard (PTES). Das Audit wird in verschiedenen Phasen durchgeührt, die nachstehend beschrieben werden.



Kick-off Meeting

Das Kickoff dient der Koordination zwischen dem Kunden und der Cybersec-ng. Ziel ist den Scope detailliert auszuarbeiten, eine Timeline und Ansprechpersonen zu definieren, mögliche Angriffszenarien zu besprechen und nicht zuletzt den Schutz der Angestellten der Cybersec-ng sicherzustellen (häufig in Form eines Schutzbriefes).

Observation (Information Gathering)

In der Observationsphase geht es um die Sammlung von Informationen über das Ziel. Dazu wird ein Assessment der physischen Sicherheit und dem Verhalten der Angestellten durchgeführt und dokumentiert. Es werden insbesondere die folgenden Bereiche berücksichtigt:

Sicherheitspersonal

Ein wichtiger und häufig erster Schritt ist die Beobachtung des Sicherheitspersonals, da dieses häufig die grösste, unmittelbare Zutrittshürde darstellt. Das Ziel der Observation ist, Bewegungsmuster, Abläufe, Ausrüstung und das generelle Verhalten des Sicherheitspersonals festzustellen.

Zutrittssysteme

Bei der Beobachtung der Zutrittssysteme geht es darum herauszufinden, wie der Zutritt in das jeweilige Gebäude stattfindet. Es wird darauf geachtet, ob und wie Badges verwendet werden, ob Schleusentüren und/oder ein Empfang/eine Rezeption vorhanden ist und ob es ungeschützte Hintereingänge beispielsweise durch Garagen und/oder “Raucherecken” gibt.

Überwachungssysteme

Ziel der Beobachtung der Überwachungssysteme ist herauszufinden, ob Sicherheitskameras vorhanden sind und wie diese ausgerichtet sind, um festzustellen, ob allenfalls blinde Stellen vorhanden sind.

CYBERSEC-NG
Swiss Cybersecurity

KONTAKT
Cybersec-ng
Grünaustrasse 1
3084 Wabern
078 729 38 39
office@cybersec-ng.ch

Verhalten der Mitarbeitenden

Hier soll festgestellt werden, wie sich die Mitarbeitenden gegenüber einer vertrauenserweckenden, aber unbekannten Person (Social Engineer) verhalten. Die Interaktionen mit den Angestellten werden, wenn möglich, audiovisuell aufgezeichnet und können in anschliessenden Awareness Trainings weiterverwendet werden. Häufig wird der Zutritt zu einem Gebäude durch die Mithilfe eines Angestellten erreicht.

Dumpster diving

Beim Dumpster Diving wird versucht an den Abfall der entsprechenden Firmen zu gelangen und diesen zu durchsuchen. Ziel hierbei ist, an sensitive, interne Informationen wie beispielsweise Identifikationsnummern oder (internen) Schriftverkehr zu gelangen und sich allenfalls mit Fachbegriffen der entsprechenden Branche vertraut zu machen. Auch wird durch das Dumpster Diving festgestellt, ob sensitive Dokumente des Angriffsziels korrekt entsorgt respektive geschreddert werden.

Erstellung & Ausführung von Angriffszenarien

Nach der Analyse, der durch die Observationsphase erhaltenen Informationen, werden potentielle Angriffsszenarien ausgearbeitet und anschliessend mit dem Kunden abgesprochen. Grundsätzlich ist eine Vielzahl von Angriffsszenarien denkbar. In der Praxis treffen wir häufig auf die folgenden Szenarien:

- Tailgating (Durchschlüpfen)
- Telefonische Angriffe
- Verkleidung als Techniker, Lieferant, Autoritätsperson, etc.
- Verteilung von mit Malware infizierten USB-Sticks auf Parkplätzen, Toiletten, vor dem Eingang, etc.
- Knacken von Schlössern und Tresoren (Lockpicking)

Reporting

Die Ergebnisse der Observations- und Ausführungsphase werden zusammen mit einer Risikobewertung (Risk, Impact) in einem Bericht zusammengefasst. Der Bericht enthält nebst einem Management Summary und einer detaillierten Beschreibung der gefundenen Schwachstellen auch audiovisuelle Elemente (siehe Verhalten der Mitarbeitenden).

Präsentation der Ergebnisse

Die Ergebnisse des Reports werden dem Kunden in Form einer Präsentation vorgestellt. Ziel der Präsentation ist, die Kommunikation der Ergebnisse sowie die Klärung von allfälligen Fragen.

Einsatzgebiete

Health Check
Sie sind Verantwortlich für die physische Sicherheit von Gebäuden und möchten überprüfen, ob Ihre Vorschriften eingehalten werden und Ihr Personal angemessen auf physische Social Engineering Angriffe reagiert. Die Resultate können in anschliessenden Awareness Trainings weiterverwendet werden.

Risk Management
Sie möchten eine Übersicht über die Schwachstellen in Ihrer physischen Sicherheit erlangen, eine entsprechende Risikobewertung durchführen und allenfalls proaktiv Gegenmassnahmen einleiten.

Angriffssimulationen zu Übungszwecken
Sie möchten Ihr Sicherheitspersonal und Ihre Angestellten schulen und dazu regelmässige Angriffssimulationen durchführen. Die periodische Durchführung von physischen Social Engineerings erhöht generell die Awareness der Mitarbeitenden und führt desweiteren dazu, dass im Ernstfall richtig reagiert und die entsprechenden Abläufe durchgeführt werden.