SOCIAL ENGINEERING

Angriffe erkennen und richtig reagieren:
In vier Schritten zum sicheren Unternehmen

Factsheet | Social Engineering

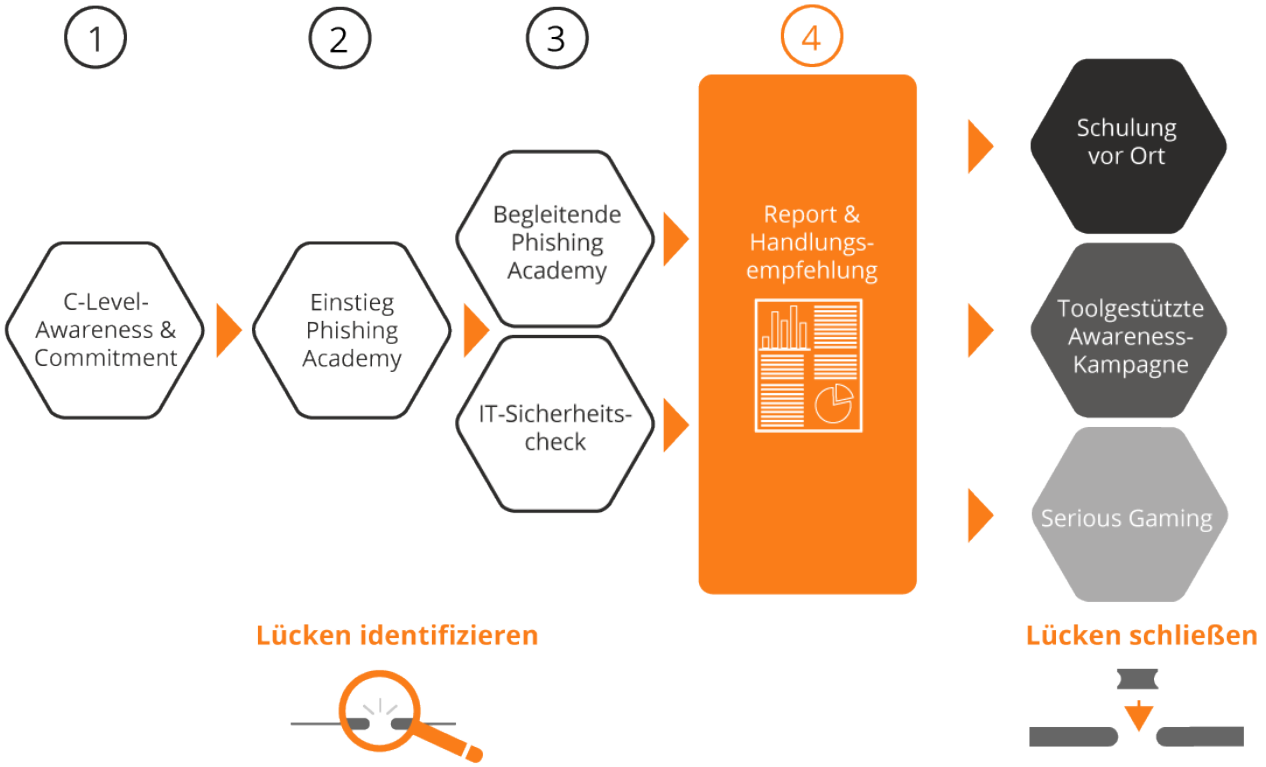
Social Engineering ist eine besonders raffinierte Form des Betrugs: Dabei werden Menschen instrumentalisiert, um sicherheitstechnisch relevante Daten in Erfahrung zu bringen.

Aktuelle Situation

Täglich werden Ihre Mitarbeiter mit Situationen konfrontiert, die leicht für Social-Engineering-Angriffe miss-braucht werden können: Beispielsweise kann bereits ein einfaches Gespräch in der Bahn oder der Anruf eines vermeintlichen Kollegen beim Help Desk dazu genutzt werden, um an sensible Daten wie Zugänge, Projekt- oder Unternehmensstrukturen zu gelangen. Zudem werden Fluten von Phishing-Mails versandt, die nur einem Ziel dienen – der Erlangung von Daten. 8 Millionen dieser E-Mails werden täglich geöffnet, jede mit dem Potenzial, ein Unternehmen durch die Unachtsamkeit seiner Mitarbeiter in den Ruin zu treiben.

In vier Schritten zum sicheren Unternehmen

Zum Schutz vor Social Engineering ist es wichtig, Vorsichtsmaßnahmen auf allen Unternehmensebenen zu ergreifen. Anhand eines Vorgehens in vier Schritten – bestehend aus einem C-Level Awareness Training für Führungskräfte, einer Phishing Academy zum Sammeln praktischer Erfahrungen im richtigen Umgang mit Phishing, einem IT-Sicherheitscheck und eines umfassenden Reports mit Handlungsempfehlungen – kann die Wahrscheinlichkeit für den Erfolg eines Angriffs signifikant gesenkt werden.



Schritt 1: C-Level-Awareness Training

Für eine erfolgreiche Zusammenarbeit ist die initiale Zustimmung von Geschäftsführung und Betriebsrat des Unternehmens notwendig. Erst danach können die verantwortlichen Abteilungen die notwendigen Maßnahmen ergreifen und nachhaltig etablieren.

Bei diesem Training erhalten Führungskräfte Werkzeuge an die Hand, um entsprechende Maßnahmen zu entwickeln und umzusetzen. Dies können beispielsweise die Beurteilung des Reputationsrisikos und des rechtlichen Risikos sein; oder eine Aufstellung dazu, welche Vermögenswerte wie geschützt werden müssen und wie Führungskräfte selbst Cyberrisiken adäquat managen können.

Das C-Level-Awareness Training findet bei Ihnen vor Ort statt und ist speziell auf die Bedürfnisse Ihres Managements ausgerichtet.

Schritt 2: Phishing Academy

In der anschließenden Phishing Academy machen Ihre Mitarbeiter erste praktische Erfahrungen bezüglich Phishings und lernen die damit verbundenen Gefahren kennen. Gleichzeitig erhalten Sie einen Überblick über die Klickraten bei leicht zu erkennenden Phishing-Mails. Anhand von Dashboards können Sie prüfen, welcher Anteil der Mitarbeiter sich für die generierten Mails anfällig gezeigt hat. Die Klickraten der Mitarbeiter auf die in den E-Mails enthaltenen manipulierten Links werden in aggregierter Form angezeigt und können über die Dauer der Academy hinweg verfolgt werden. So können Sie nachvollziehen, wie stark die Klickraten während des Verlaufs der Maßnahme sinken.

Schritt 3: IT-Sicherheitscheck und begleitende Phishing Academy

Der syracom IT-Security-Check verschafft Ihnen einen Überblick über die aktuelle Situation der IT-Sicherheit Ihres Unternehmens und zeigt akute Handlungsbedarfe auf. Zeitgleich wird zur Verstärkung des Trainingseffekts eine weiterführende Phishing Academy mit erhöhtem Schwierigkeitsgrad gestartet.

Schritt 4: Erstellung Report & Handlungsempfehlungen

Die Ergebnisse aller Maßnahmen werden eingeordnet und um Handlungsempfehlungen ergänzt. Die Ergebnisse präsentieren wir Ihnen persönlich vor Ort. Wir zeigen auf, wie Sie Risiken in Ihrem Unternehmen minimieren können. Sie erhalten zusätzlich einen umfassenden Report zur Verfügung gestellt.

Das Ergebnis: Nachhaltige Sicherheit

syracom setzt zur Behebung von Sicherheitslücken auf eine Kombination aus verschiedenen Lösungsbausteinen: Schulung vor Ort, dem Einsatz von Serious Games und eine Plattform mit individuell konfigurierbaren Schulungsinhalten. Über Serious Games erwerben Ihre Mitarbeiter auf unterhaltsame Weise Wissen und praktische Fertigkeiten im Umgang mit Social Engineering Angriffen sowie über IT Security im Allgemeinen. Diese Methode bietet sich an, da Mitarbeiter intrinsisch motiviert werden und damit ihr Eigenantrieb gefördert wird.

Die verschiedenen Bausteine orientieren sich an dem zuvor identifizierten Handlungsbedarf und werden genau auf Ihre Bedürfnisse abgestimmt. Auf allen Ebenen wird ein Problem- und Verantwortungsbewusstsein geschaffen, welches auch langfristig funktioniert – vom C-Level bis zu den Spezialisten in den Fachabteilungen.

Warum syracom?

syracom verfügt über langjährige Erfahrung im Bereich IT Security. Mit einem umfassenden Partnernetzwerk bündelt das Beratungshaus optimal Experten und Knowhow. syracom berät Sie unabhängig bei der Lösungsfindung und versteht sich als ganzheitlicher Begleiter bei deren Umsetzung. Sie profitieren von umfassendem Security-Wissen in unserem vier Säulen Modell, das neben Social Engineering weitere essenzielle Bausteine zur Erhöhung der Informationssicherheit umfasst.

syracom

Frank Hofmann

Leiter Themenbereich
IT-Security

syracom AG
Otto-von-Guericke-Ring 15
65205 Wiesbaden (Germany)
Fon: 06122 9176 0
frank.hoffmann@syracom.de
www.syracom.de