InfoGuard
SWISS CYBER SECURITY

SOCIAL ENGINEERING AUDIT

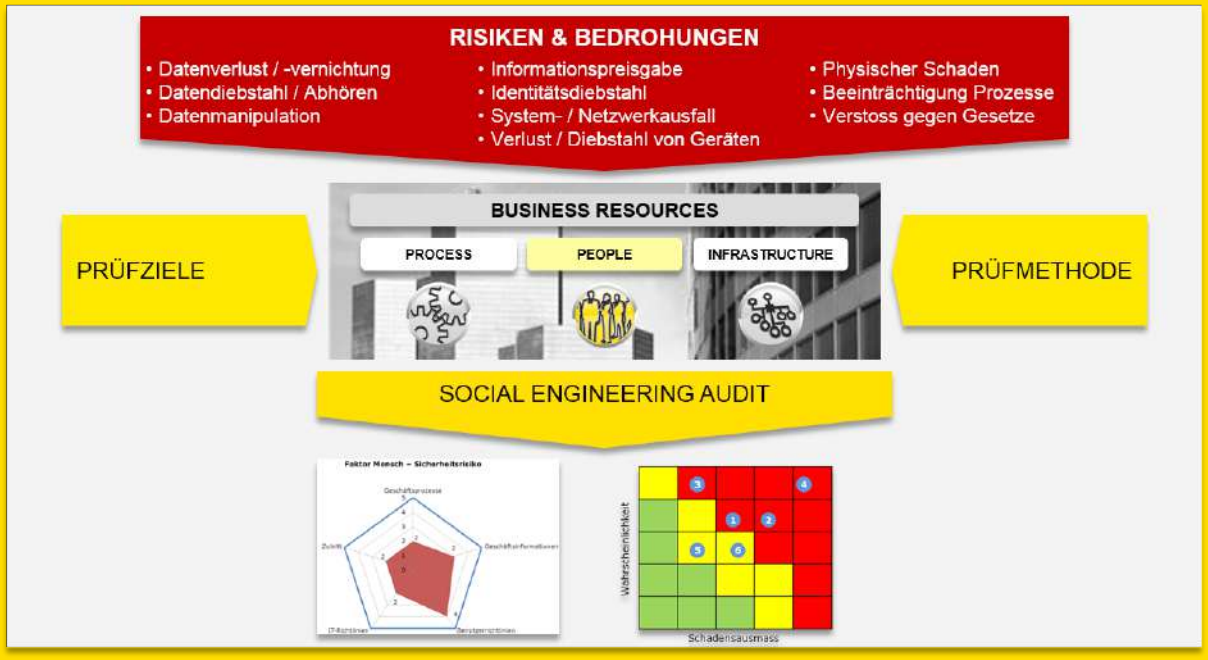
Risikofaktor «Mensch» systematisch überprüft.

VERIFIKATION DES SICHERHEITS-VERHALTENS IHRER MITARBEITER

Mit unseren Social Engineering Audits überprüfen wir nicht einzelne Personen, sondern verifizieren anonymisiert die Einhaltung von sicherheitsrelevanten Geschäftsprozessen und Richtlinien sowie den Umgang mit sensiblen Informationen. Alle Prüfziele und -Methoden werden vorgängig mit dem Auftraggeber besprochen und durch die Verantwortlichen genehmigt.

Je nach Prüfziel und Zielgruppe setzen wir unterschiedliche Prüfmethoden und Angriffsarten des Social Engineering ein. Diese reichen vom persönlichen Kontakt mit der Zielperson per Telefon oder physisch vor Ort, über den elektronischen Weg über E-Mail, Chat oder Social-Network-Plattformen, bis hin zur postalischen Kontaktaufnahme. Aber auch die gezielte Abgabe von manipulierten USB Speichermedien oder die systematische Datenanalyse auf dem Internet sowie die Auswertung von Logfiles und Systeminformationen gehören dabei zum Angriffsrepertoire der InfoGuard.

- **Deckt Schwachstellen im Umgang mit sensiblen Geschäftsinformationen auf.**
- **Gezielte Überprüfung der Einhaltung von sicherheitsrelevanten Geschäftsprozessen, Benutzerrichtlinien, IT-Sicherheitsrichtlinien und Zutrittsregelungen.**
- **Liefert ein Stärken-Schwächen-Profil gegenüber ISO 27002 und beschreibt konkrete Massnahmen zur Risikominimierung.**



Prüfziele

- Sicherheitsrelevante Geschäftsprozesse
- Umgang mit sensiblen Geschäftsinformationen
- Einhaltung von IT-Sicherheitsrichtlinien
- Einhaltung von Zutrittsrichtlinien

Prüfmethoden

- Information Gathering
- Persönlicher Kontakt
- Interviews
- Phishing und Malware
- Analyse von IT-Systemen
- Vor Ort Inspektionen

Kommunikationswege

- Persönliches Gespräch
- Briefpost
- Telefon und SMS
- E-Mail und Internet
- Social-Network-Plattformen

Systematisches Vorgehen von der Bedrohungsanalyse, über die Planung und Durchführung bis zur Risikobewertung und Massnahmenempfehlung.

Social Engineering Audit in sechs Schritten

1 Bedrohungsanalyse und Definition der Prüfziele
Die Basis für die Überprüfung bildet eine spezifische Bedrohungsanalyse, mit Gefahren, Erfolgschancen und Risikoklassen. Dabei betrachten wir Risiken wie Datenverlust, -diebstahl oder -manipulation, Identitätsdiebstahl und Verstoss gegen firmeninterne Prozesse oder Gesetzesbestimmungen um nur einige zu nennen. In einem Meeting werden die Prüfziele definiert, das Vorgehen terminiert und die Verantwortlichkeiten und Rahmenbedingungen geklärt.

2 Planung der Überprüfung und Ausarbeitung der Prüfmethoden
In diesem Projektschritt werden die relevanten Benutzerweisungen und vorhandenen Security-Baselines des Auftraggebers gesichtet. Um zu erfahren, was erlaubt oder nicht erlaubt ist, analysieren wir die vorhandenen Richtlinien und führen ergänzend Gespräche. Anschliessend werden die effektivsten Prüfmethoden ausgearbeitet, geplant und in einem detaillierten Drehbuch festgehalten. Dieses wird von den verantwortlichen Personen des Kunden geprüft und genehmigt.

3 Überprüfung
Als zentrale Phase folgt nun die Überprüfung mit den definierten Tests. Dieser Schritt umfasst immer einen Mix aus verschiedenen Prüfmethoden. Treten dabei schwerwiegende Mängel auf, wird der Kunde sofort informiert, so dass allfällige Sofortmassnahmen umgehend umgesetzt werden können.

4 Workshop – Risikobewertung
Die Ergebnisse der Prüfungen werden mit dem Kunden in einem Workshop besprochen. Dabei werden die ermittelten Schwächen und die wesentlichen Risiken zur Informationssicherheit, insbesondere zum «Faktor Mensch» interpretiert und bwertet, um im letzten Schritt den Bericht abzuschliessen.

5 Bericht mit Bewertung & Empfehlungen
Sämtliche Erkenntnisse aus den Analysen und dem Workshop werden im Gesamtbericht zusammengetragen und durch ein Stärken-/Schwächen-Profil dem internationalen Standard für IT-Sicherheit ISO 27001 gegenüber gestellt. Die erkannten Schwachstellen werden bewertet und mit Empfehlungen versehen. Die konkreten Massnahmenempfehlungen sind dabei im Detail beschrieben und gemäss der Risikoeinschätzung priorisiert.

6 Abschlussbesprechung
Der Schlussbericht wird im Rahmen einer Präsentation mit dem Auftraggeber besprochen. Für das Management wird eine umfassende und aussagekräftige Zusammenfassung über die Projektdurchführung, die Erhebungsergebnisse und über die daraus resultierenden Sicherheitsmassnahmen erstellt. Selbstverständlich sind wie dem Kunden bei der Umsetzung gerne behilflich.

SOCIAL ENGINEERING AUDIT – NUR EIN BESTANDTEIL VON UMFASSENDEN SICHERHEITS-AUDITS UND -REVIEWS

Ihre Geschäftsprozesse funktionieren nur, wenn stets die richtigen Informationen zur richtigen Zeit am richtigen Ort vorzufinden sind. Vertraulichkeit, Integrität und Verfügbarkeit der Informationen spielen dabei eine bedeutsame Rolle.

InfoGuard bietet eine unabhängige Überprüfung Ihrer Informationssicherheit. Dabei zeigen wir auf, welche organisatorischen, technischen und personellen Schwachstellen in Ihrem Unternehmen vorliegen und wie Sie diesen begegnen können.

Unsere Dienstleistungen umfassen die Bereiche:

- Security Audit nach ISO 27001/27002
- GAP-Analyse hinsichtlich einer ISO 27001-Zertifizierung
- System- und Architektur-Review
- Penetration Test nach OSSTMM
- Vulnerability Scan
- Social Engineering Audit

Ihre Sicherheit ist unser Ziel –
wir analysieren und optimieren Ihr Sicherheitssystem!

InfoGuard – Der Schweizer Cyber Security Experte

InfoGuard ist ein Schweizer Experte für umfassende Cyber Security und innovative Netzwerklösungen. Sie profitieren von unserer Erfahrung, Professionalität und Zuverlässigkeit im Audit, in der Beratung, Architektur und Integration führender Netzwerk- und Security-Lösungen. State-of-the-Art Cloud-, Managed- und Cyber Defence-Services erbringen wir aus dem ISO 27001 zertifizierten InfoGuard Cyber Defence Center in der Schweiz.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz
Telefon +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Schweiz
Telefon +41 31 556 19 00

INFOGUARD.CH