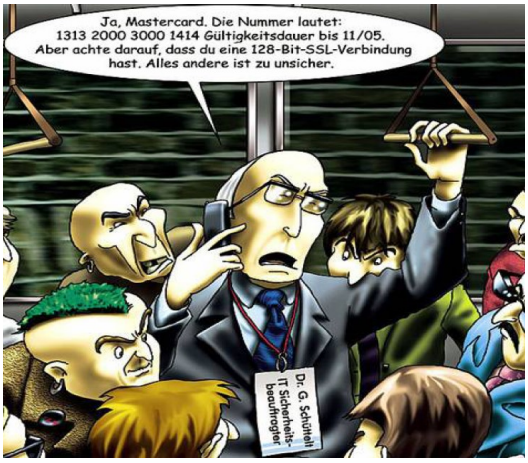
Sicherheits-Sensibilisierung

- **Welche Angriffe sind über die "Schwachstelle Mensch" zu erwarten?**
- **Das Fehlverhalten der Mitarbeitenden ist das grösste Risiko, aber auch Ihre grösste Chance auf mehr Sicherheit.**
- **Wir machen Ihre Sicherheit messbar.**
- **Wir zeigen Ihnen eine kostengünstige und wirksame Security-Awareness-Aktion.**



Ihre Situation

Cyberattacken beginnen meistens mit einem Anhang in einer Phishing E-Mail. Der unkorrekte, unachtsame oder nachlässige Umgang der Mitarbeitenden mit vertraulichen Informationen zählt zu den grössten Risikofaktoren für Unternehmen. Angezeigt ist daher eine grundlegende Sensibilisierung aller Mitarbeitenden auf ein sicherheits- und verantwortungsbewusstes Denken und Handeln in der Unternehmenstätigkeit.

Unser Angebot

Eine erfolgreiche Sensibilisierung besteht aus verschiedenen Phasen. Diese beginnen mit dem Wecken des Interesses für das Thema. Der Mitarbeitende möchte dann von sich aus wissen, warum verschiedene Massnahmen zur Informationssicherheit eingeführt werden und wird danach das Verständnis für diese erlangen. Weil er nun versteht und akzeptiert, wird er entsprechend handeln. Am Anfang vielleicht noch mit Aufwand und Mühe, bald aber selbstverständlich und aus Gewohnheit.

Die Stärkung des Sicherheitsbewusstseins führt zum Wachstum der Sicherheitskultur im Unternehmen und verbessert die Akzeptanz der Informationssicherheit und des Datenschutzes, so dass diese zu einer Selbstverständlichkeit und zum Bestandteil der Firmenkultur wird.

Ihr Nutzen

- Stufengerechte Sensibilisierung der Mitarbeitenden
- Sensibilisierung des Managements
- Festigung das Sicherheitsbewusstseins
- Vermittlung des Sicherheitswissens
- Förderung des korrekten Sicherheitsverhaltens
- Sehen—verstehen—handeln

„Die Schwachstelle Mensch stellt das grösste Risiko dar!

Was können Sie von uns erwarten?

Um eine bleibende Verhaltensänderung zu bewirken, müssen die Informationen regelmässig aufgefrischt und aktualisiert werden. Die betroffene Person soll sich direkt angesprochen fühlen und sich ihrer wichtigen Rolle auf dem Weg zum Erfolg bewusst sein.

- Erstellen eines Security-Awareness Konzeptes
- Erstellen, planen und Durchführen von wirksamen Security-Awareness-Aktionen in Ihrem Unternehmen
- Überprüfen der Lieferantenkette in Bezug auf mögliche Schwachstellen.
- Durchführen von Live-Hacking Anlässen
- Die Funktionsweise des Social-Engineering sowie der Schwachstelle Mensch aufzeigen
- Durchführen von fingierten Phishing-Attacken auf Ihr Unternehmen

Informationssicherheit neu definiert

angemessen—konkret—auf den Punkt gebracht

SERVICE QUALITÄT KOMPETENZ
ÜBER 10 JAHRE FÜR SIE DA

SIDLER
Information Security

Holzhäusernstrasse 5a
6331 Hünenberg / Zug

Tel. 041 781 57 72
www.sidler-security.ch
info@sidler-security.ch