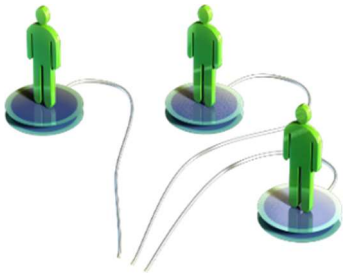
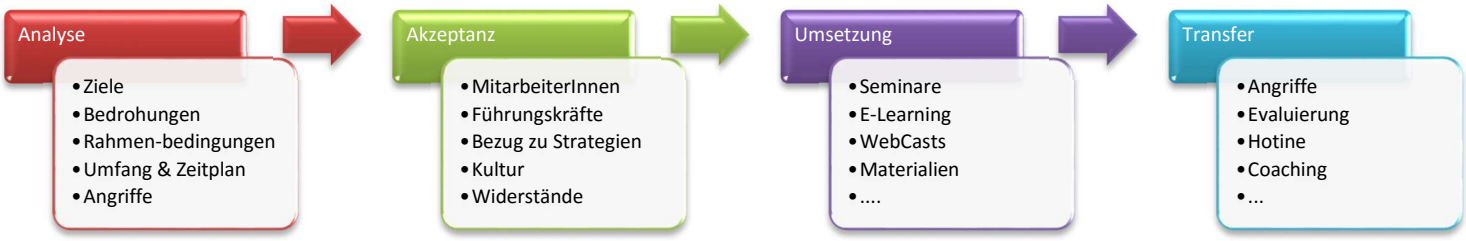
>>Security Awareness Programme

EGOS! the education company

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren und Würmer bedrohen Unternehmens-Assets von außen, Sozial Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den Security Gedanken in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne Diese zu behindern.



Möglicher Ablauf zur Einführung



Risikoanalyse (Initial Workshop): Es werden mögliche Bedrohungen erhoben, Zeitrahmen, Methoden sowie budgetäre Mittel festgelegt. Die Unternehmenskultur ist bei der Auswahl der Aktivitäten zu beachten.

Social Engineering Angriffe: Mögliche Aktivitäten könnten illegales Betreten der Organisation, Anrufe, Mails, Platzierung von Fremdgeräten etc. sein. Zusätzlich werden die Security Policies sowie sonstige relevante Richtlinien und Dokumente geprüft.

Security Awareness Programm: Die Ergebnisse der Angriffe werden ausgewertet. Basierend auf den Erkenntnissen wird ein passendes Programm erstellt:

Transfersicherung: Einige Zeit nach Durchführung der Aktivitäten werden erneut ähnliche *Angriffe* wie am Beginn durchgeführt. Die Ergebnisse der Angriffe werden korreliert und die entsprechenden Schritte für ein *nachhaltiges Programm* gesetzt.

Richtlinien	Training	Kommunikation	Marketing
•Policies	•Seminare/Workshops	•Veranstaltungen	•POI's nutzen
•Compliance	•Webinare/Web-Cast's	•Videos	•Broschüren
•Datenklassifizierung	•E-Learning	•Infoportale	•Give Aways
•Rollenbeschreibungen	•IT-Team	•Intranet/Foren	•Screensaver
•Arbeitsverträge	•Datenschutzbeauftr.	•Wiki's / Blogs	•Firmenzeitungen
•Anweisungen	•Sicherheitsbeauftr.	•Mobile App's	•Infoscreens
	•Führungskräfte	•Mails/Umfragen	•Poster

Training der MitarbeiterInnen in Seminaren

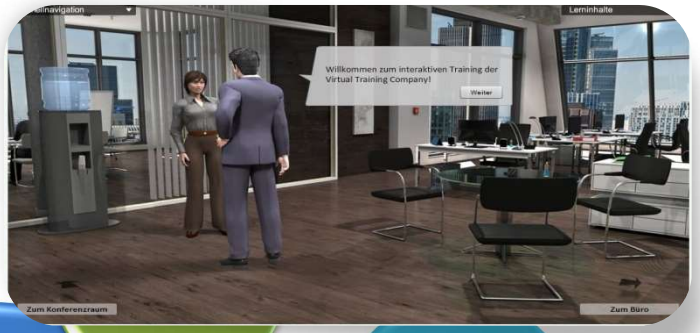
- Informationssicherheit für Anwende: http://www.egos.co.at/go/agenda/4238
- Datenschutz I: Grundlagen: http://www.egos.co.at/go/agenda/8079
- Datenschutz II: Praxisumsetzung in Organisationen: http://www.egos.co.at/go/agenda/8080
- Datenpannen: Bedrohung und Handling: http://www.egos.co.at/go/agenda/7462
- Betrug und kriminelle Aktivitäten in der IT: http://www.egos.co.at/go/agenda/7461

u.v.a.m.

Training der MitarbeiterInnen mit E-Learning

Ein nachhaltiges Security Awareness Programm unterstützen wir mit der Lernsoftware Virtual Training Company. Die 3D-Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen. Dabei navigieren die Mitarbeiterinnen nachweislich durch ein virtuelles Unternehmen, in welchem kontextbezogen verschiedene Inhalte mit Hintergrundinformationen, Beispielen und Trainingsszenarien untergebracht sind.

Schauplätze sowie die Lerninhalte der Virtual Training Company sind auf Wunsch an die Optik und Corporate Identity des Unternehmens anpassbar und voll konfigurierbar. Die 3D-Software ist die derzeit innovativste Lösung, um Security Awareness nachhaltig zu vermitteln und das Sicherheitsbewusstsein der MitarbeiterInnen entscheidend zu stärken.



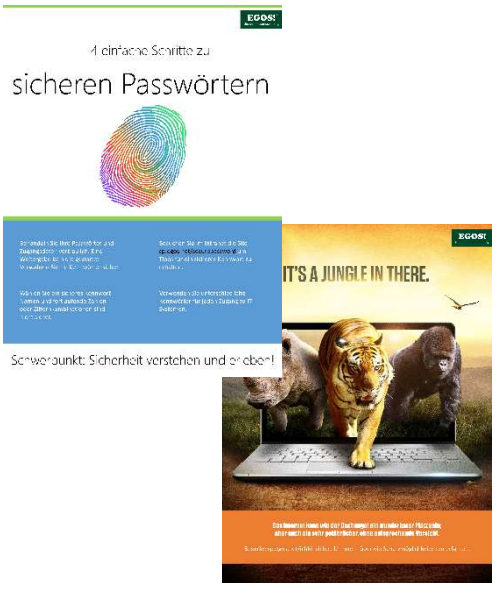
Mögliche Intensität eines Programms

Schwerpunkt Compliance	Awareness & Change	Nachhaltigkeit
Das geplante Programm konzentriert sich auf Anforderungen für Compliance oder Zertifizierungs-Audits. Trainings werden sporadisch angeboten. Die Wichtigkeit von Sicherheitsrichtlinien für den Schutz von Unternehmensdaten ist Mitarbeitern zwar bekannt, wird aber nur wenig umgesetzt.	Das Programm hat große Auswirkungen auf die Unternehmensziele und fokussiert die Trainingsmaßnahmen darauf. Neben regelmäßigen Trainingsmaßnahmen werden laufen Maßnahmen zur Festigung der Richtlinien durchgeführt. Die Inhalte werden in unterschiedlichen Kanälen kommuniziert sodass das Verhalten von Mitarbeitern am Arbeitsplatz, zu Hause und auf Reisen positiv beeinflusst wird. Als Ergebnis verstehen Mitarbeiter die Sicherheits-Richtlinien, befolgen diese und tragen aktiv zur Umsetzung bei.	Das Programm definiert Prozesse im Rahmen einer langfristigen Umsetzung. Als Minimum werden ein jährliches Review und eine Aktualisierung der Inhalte und der Kommunikationskanäle durchgeführt. Sicherheits-Richtlinien sind Teil der Unternehmenskultur und sind auf dem aktuellen Stand.
• Definition der Ziele • Welche Standards muss das Unternehmen erfüllen? • Welche Anforderung an Security Awareness fordert der Standard? • Welche Besonderheiten sind zu beachten? • Entwicklung von Trainingsinhalten und evtl. begleitenden Maßnahmen • Protokollierung der Trainingsergebnisse	• Definition der Projektbeteiligten/Entscheider • Erhebung des IST-Zustandes hinsichtlich IT-Security; Evtl. Security-Check • Erstellen eines Projektplans mit den Verantwortlichen: Kostenrahmen, Anwendungsbereiche, Themengebiete, Meilensteine und Annahmen • WER ist die Zielgruppe des Programms? z.B.: MitarbeiterInnen, Service-Desk, IT Administratoren, Entwickler, Führungskräfte • WELCHE Inhalte sind für welche Zielgruppe relevant? Erstellen Risikomatrix / Priorisierung Themenbereiche • WIE wird der Inhalt kommuniziert? Wesentlich ist die Unterscheidung in Vermittlung von Inhalten und Transfermethoden. Inhaltsvermittlun: Präsentationen, Workshops, Webinare, E-Learning Transfersicherung: Videos, Postings, Newsletter, Poster, etc.. • Erstellen eines Durchführungs- / Zeit-plans	• Definition der Zeitpunkte an denen eine Überarbeitung erfolgt • Auflistung von neuen oder geänderten Technologien, Bedrohungen, Geschäftsanforderungen oder geänderten Standards • Erhebung der Kennzahlen • Umfrage bei Mitarbeitern, welche Inhalte am besten angekommen sind und wo Änderungsbedarf besteht • Prüfung aller Dokumente und Inhalte die kommuniziert werden. • Aktualisierung der zu ändernden Inhalte und Dokumente • Aktualisierung der Projektplans • Kommunikation der geänderten Inhalte

Mögliche Messbarkeit eines Programms

Das Programm setzt auf Kennzahlen, die laufend kontrolliert werden:

- Definition der Kennzahlen, die gemessen werden sollen
- Dokumentation wie und wann die Messwerte erhoben werden.
- Wer wird über die Messwerte informiert? Wo werden Diese dargestellt?
- Anzahl Personen mit Phishing Attacken
- Anzahl der gemeldeten Security Incidents
- Anzahl der infizierten Systeme
- Anzahl Personen, die das Awareness Training absolviert haben
- Anzahl unsichere Kennwörter u.v.a.m.



Investitionsparameter

Maßnahme	Kosten pro Maßnahme	Multiplikator
Initial-Workshop - Festlegen Themenbereiche - Auswahl Kommunikation und Terminplan/Häufigkeit - Bereitstellung von Werkzeugen - Festlegen der Kennzahlen	€ 1.600,-	pro Tag
Simulation von Social Engineering Angriffen (20 Angriffe)	€ 2.500,-	pro Simulation
Erarbeiten Security Richtlinien (ca. 1,5 Tage)	€ 1.200,-	pro Tag
Erarbeiten Dokumentklassifizierung (ca. 1,5 Tage)	€ 1.200,-	pro Tag
Vorstellung des Programms bei Führungskräften (ca. 0,5 Tage)	€ 800,-	pro Tag
Security Awareness Seminare für AnwenderInnen (ca. 1 Tag)	€ 1.200,-	pro Tag
Security Awareness Seminare für IT MitarbeiterInnen (ca. 2 - 3 Tage)	1.600,-	pro Tag
Security Awareness E-Learning Lizenzen	ca. € 5,-	pro Mitarbeiter
Erstellen Broschüre, Aufsteller, 2xA4 Seite (2 Varianten / 1 Review) Input: Themenbereich, 3-5 Stichworte, Basis-Design/Corporate Design	€ 350,-	pro Dokument
Druck-Kosten Broschüre, Aufsteller	ca. € 10,-	pro Broschüre
Erstellen Poster in A1/HD oder Rollup (2 Varianten / 1 Review) Input: Themenbereich, 3-5 Stichworte, Basis-Design/Corporate Design	€ 350,-	pro Poster
Druck-Kosten Poster Größe A1 ohne Rahmen	ca. € 50,-	pro Poster
Produktions-Kosten Rollup	ca. € 150,-	pro Rollup
Vorschlag und Auswahl von Giveaways (2-3 Vorschläge)	€ 350,-	pro Giveaway
Erstellen Artikel für Intranet / Firmenzeitung (Größe ca. ½ Seite) Input: Themenbereich, 3-5 Stichworte, Basis-Design/Corporate Design	€ 400,-	pro Ausgabe
Gestaltung Newsletter Kampagne Input: Themenbereich, 3-5 Stichworte SMTP Zugang erforderlich	€ 400,-	pro Newsletter
Erstellen Blog-Eintrag Input: Themenbereich, 3-5 Stichworte Remote-Zugang zu Blog erforderlich	€ 400,-	pro Artikel
Erstellen Awareness Videos	n. Aufwand	pro Video

Alle Preise verstehen sich als Richtwerte exkl. USt. und evtl. anfallender Reisekosten von TrainerInnen / BeraterInnen