

Security-Awareness in der Praxis



KA-IT-Si-Event
22.09.2011

Beobachtungen

Beobachtungen

- ◆ **Mitarbeiter sind häufig (Mit-) Verursacher von Schäden**
 - Wahl ungeeigneter Passworte, Weitergabe, Hinterlegung
 - Anfälligkeit für „Social Engineering“
 - Nachlässiger Umgang mit sensiblen Daten (Laptop)

- ◆ **Mitarbeiter unterschätzen den Wert von Informationen**
 - „Wen soll das wohl interessieren?“
 - Ursache: Unkenntnis der Bedeutung von Informationen für Dritte

- ◆ **Risikoannahmen erscheinen „realitätsfern“**
 - „Bei uns ist ja noch nie etwas passiert.“
 - Ursache: Vorfälle und Schäden werden nicht kommuniziert
 - „So schlimm ist das alles doch gar nicht.“
 - Ursache: Unkenntnis über Hintergründe, Methoden, Tools und Vorgehensweisen von Angreifern

Beobachtungen

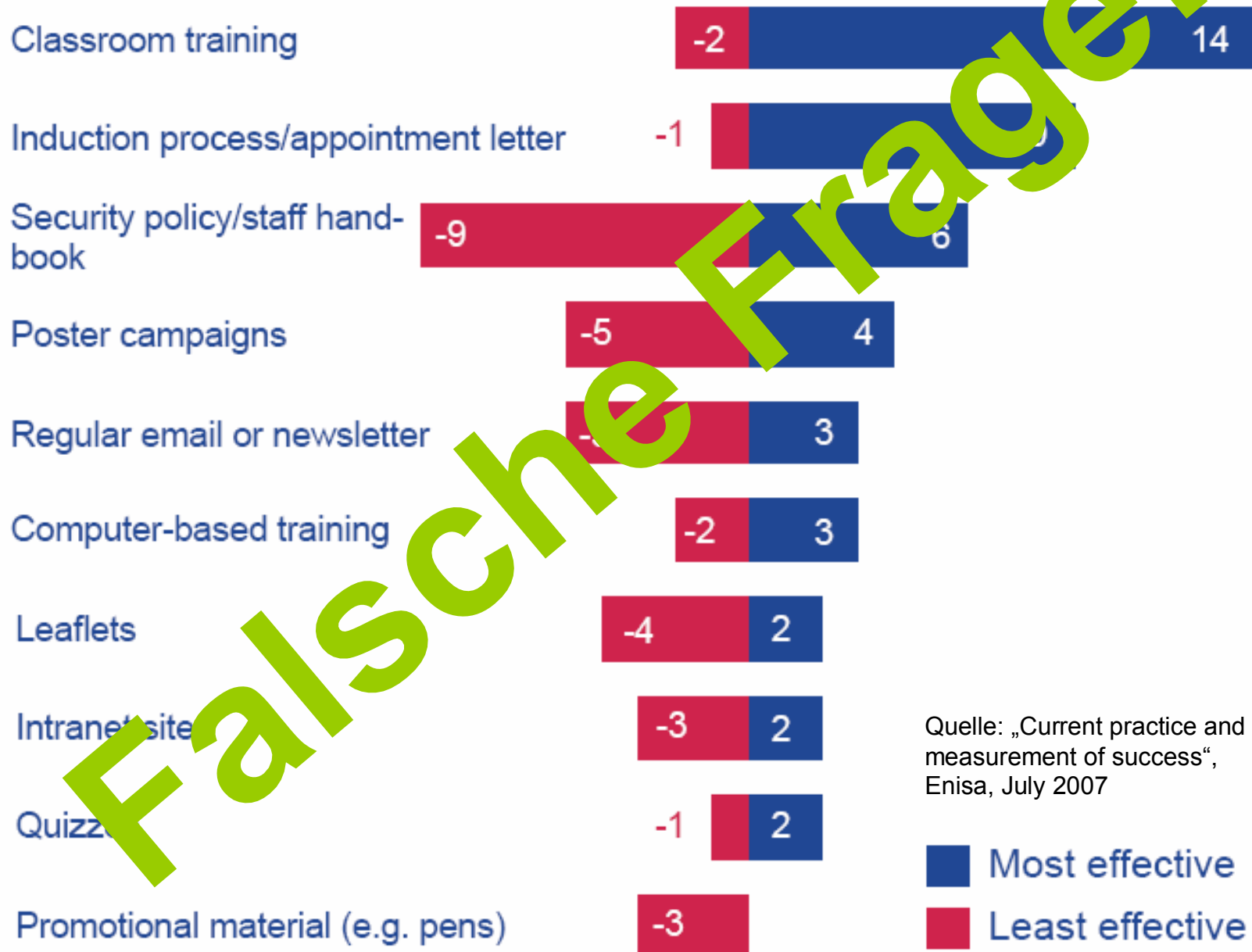
- ◆ **Schutzmaßnahmen werden als Behinderung empfunden**
 - „Da hat bestimmt wieder der Virens Scanner dazwischengefunkt“
 - Stimmt meistens nicht
 - Ursache: Schutzmaßnahmen verlängern Prozesse; Wirkung wird „kleingeredet“, Maßnahme nicht motiviert
- ◆ **Verantwortung wird Dritten zugewiesen**
 - „Wozu haben wir eigentlich eine IT-Abteilung?“
 - Es ist immer gut, einen anderen Verantwortlichen zu finden
 - Ursache: Bedeutung des eigenen Verhaltens wird übersehen
- ◆ **Regeldurchsetzung wird meist technisch erzwungen**
 - „Für das Problem gibt es (bestimmt) ein Tool“
 - Technische Schutzmaßnahmen überwiegen
 - Ursache: Ingenieurdenken und (naiver) Technikglaube

Aufgabenstellung

Vermittlungsziele

- ◆ **Ziel: Verhinderung von Fehlverhalten, das unerwünschten Informationsabfluss bewirkt oder begünstigt**
- ◆ **Was sind schützenswerte Informationen?**
 - **Transparente und möglichst eindeutige Datenklassifikation**
- ◆ **Wo geben Mitarbeiter schützenswerte Informationen preis?**
 - **Kommunikation in der Öffentlichkeit**
 - **Nutzung von IT-Systemen in der Öffentlichkeit**
- ◆ **Wo geben Mitarbeiter freien Zugang zu Informationen?**
 - **Schreibtisch, Ablage, Dokumente in öffentlichen Verkehrsmitteln**
- ◆ **Wo „verlieren“ Mitarbeiter schützenswerte Informationen?**
 - **Mobile Geräte (Laptop, Smartphone, Handy)**
 - **Entsorgung von Papierdokumenten, Speichermedien (USB)**

What techniques have proved effective at raising information security awareness?



Fünf Awareness-Grundsätze

Grundsatz Nr. 1

**Awareness braucht
Verständnis.**

Wie sicher ist Ihr Passwort?

Passwort	2003	2007
----------	------	------

Vier Zeichen

15u1	0h 1m 39s	0h 0m 0s
h2TU	0h 1m 40s	0h 0m 1s
G6_W	0h 1m 41s	0h 0m 1s

Sechs Zeichen

-f\$2Ms	3h 19m 17s	0h 17m 38s
cL9ge!	15h 13m 9s	0h 33m 57s
-6nC3\$	16h 11m 26s	0h 37m 19

Wie sicher ist Ihr Passwort?

- ◆ RainbowCrack, Aldi-PC, Grafikkarte (ca. 1 T€)

2011

Vier Zeichen

0,3 ms

Sechs Zeichen

3,4 s

Acht Zeichen

6,7 h

Ein paar Testfragen ...

- ◆ **Wie viele neuartige Viren, Würmer und Trojaner werden täglich entdeckt?**
- ◆ **Haben Sie schon einmal einen echten Trojaner „in Funktion“ erlebt?**
- ◆ **Wissen Sie, welchem Zweck Passwortwechsel dienen?**

Grundsatz Nr. 2

**Awareness braucht
klare Regeln.**

Grundsatz Nr. 3

**Awareness braucht
eine starke Marke.**

Grundsatz Nr. 4

**Awareness braucht
Tools.**

Tools

◆ Tipps für's Private

- Sicherheitsmaßnahmen zu Hause erhöhen die Sensibilität

◆ Merktzettel

- Zur angemessenen Reaktion auf Anfragen und Anrufe Unbekannter
- Zur Klassifikation von Dokumenten bzw. Informationen
- Zum Umgang mit Passwörtern

◆ Benutzerfreundliche (IT-) Hilfsmittel

- „One-Click“-Verschlüsselungslösung
- Sicherer Passwort-Speicher
- Polarisationsfilter für Laptops

◆ Simulierte Vorfälle

- Krisenreaktionsübung
- Live-Hacking
- Social-Awareness-Attacken

Grundsatz Nr. 5

**Awareness braucht
Vorbilder.**

Aufgabe der Führungskräfte

- ◆ **Vermittlung der Verhaltensrichtlinien**
- ◆ **Einfordern der Regeleinhaltung**
- ◆ **Vorbildliches eigenes Verhalten**
- ◆ **Sanktionierung von Verstößen**
(unmittelbar und ohne Ansehen der Person)
- ◆ **Steigerung der Mitarbeiterzufriedenheit (= Loyalität)**
- ◆ **„Patenschaft“ für die Kampagne**
(Zitate, E-Mail-Schreiben, Video-Ansprache, ...)

Fazit

Erfolgsfaktoren

◆ Erfolgreiche Awareness-Initiativen haben

- ein **messbares Ziel**
- eine einheitliche **Strategie**
- einen passgenauen **Zuschnitt** auf die Unternehmenskultur
- die **Überzeugung** der Mitarbeiter zum Ziel
- die **Unterstützung** des gesamten Managements
- verzahnte Einzelmaßnahmen mit strukturiertem Aufbau
- eine verbindende **Klammer** (Key Visual, Brand, Claim)

◆ Awareness braucht

- **Verständnis.**
- **einfache Regeln.**
- **eine starke Marke.**
- **Tools.**
- **Vorbilder.**



secorvo

security consulting

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

NEU

Das Begleitbuch zum T.I.S.P.

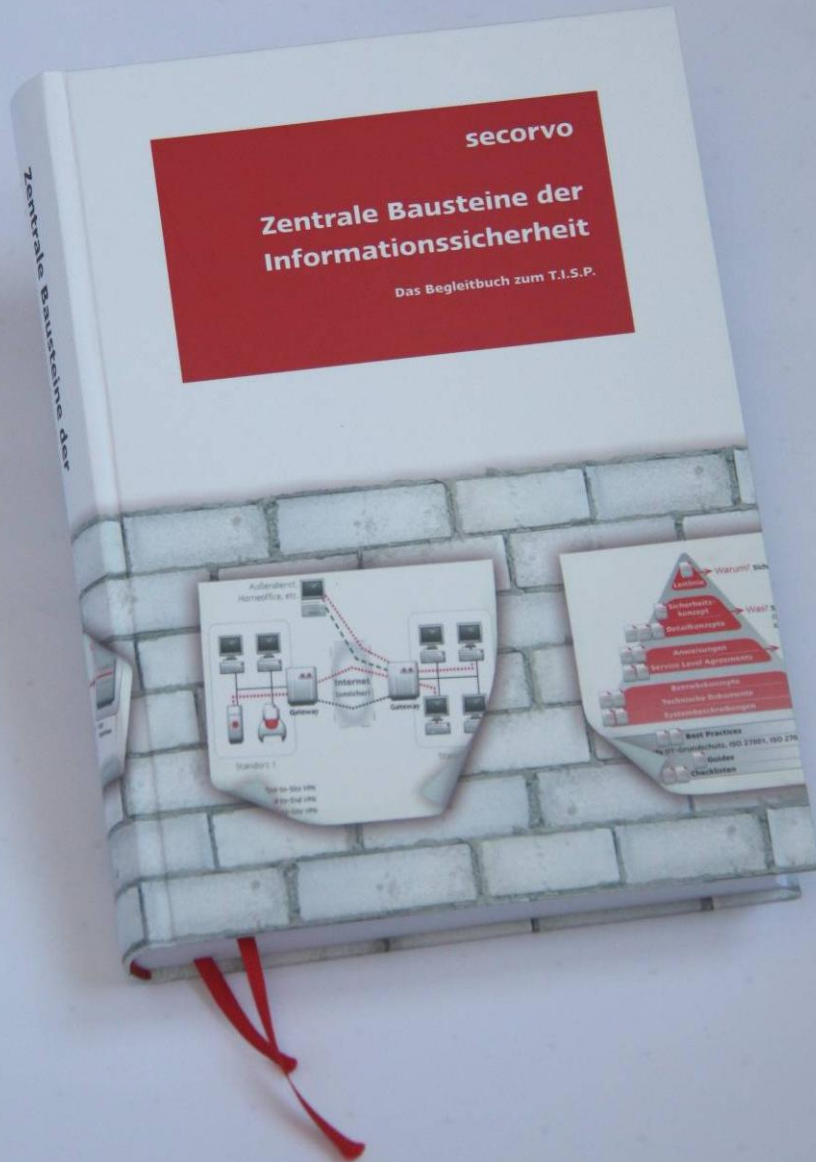
Gebundene Ausgabe

520 Seiten

ISBN: 978-3-942594-08-0

Preis: 79,95 EUR

www.tisp.de

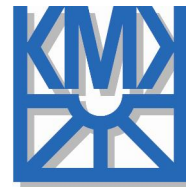


Die Partner der IT-Si

Karlsruher IT-Sicherheitsinitiative



Die Unterstützer der



Karlsruher
Messe- und
Kongress-
GmbH



Medienpartner

