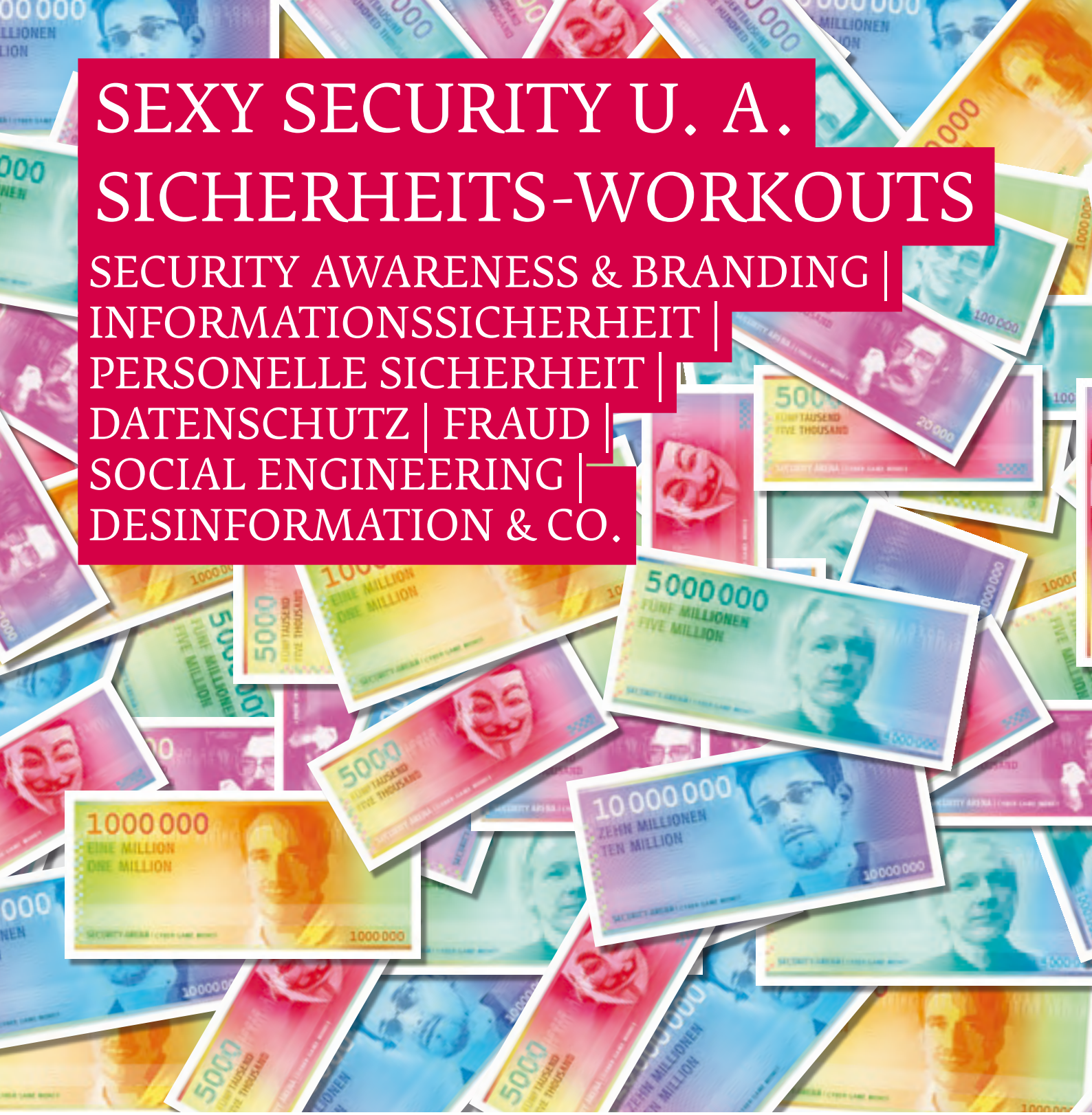


IT-Sicherheitspreis NRW 2007
für askit
by known-sense

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen
Sicherheitspreis Baden -Württemberg 2011 für Cytec-Audio-Podcasts

Information Security Forum
Most innovative Awareness Campaign 2013: „SECURITY PARCOURS“ by T-Systems – supported by known_sense

Outstanding Security Performance Award (OSPA) 2015: „Herausragende Initiative für Sicherheitsschulungen“ für „SecurityArena“ by known_sense

known_sense
awareness you can touch.

NACHHALTIGE AWARENESS – WARUM IST ES SO WICHTIG, MITEINANDER ZU SPRECHEN?

Security-WorkOuts – die neuen Seminarangebote von known_sense

Nach zahlreichen Kampagnen für namhafte Unternehmen, Einsichten aus unseren Studien und Erkenntnissen unserer TAKE-AWARE-Kongresse, wollen wir Ihnen und Ihren Mitarbeitern unsere vielfältigen Erfahrungen im Rahmen unserer neuen und innovativen Security-WorkOuts vermitteln.

Warum keine „normale Schulung"?

Anders als bei klassischen IT- bzw. Security-Seminaren und -Schulungen stehen nicht die technischen Aspekte im Vordergrund, sondern die Menschen. Und wie immer bei known_sense greifen wir auch in den WorkOuts vor allem die spezifischen Widersprüche und Widerstände in Bezug auf die einzelnen Themen auf – eben die psychologische Seite der Sicherheit – und versuchen technische und rechtliche Notwendigkeiten mit den menschlichen Eigenarten und Bedürfnissen in Einklang zu bringen. Wir bedienen uns dabei wie gewohnt auch in den WorkOuts kreativer didaktischer Methoden und bieten einen bewährten Mix aus erfolgreichen Instrumenten. Erprobte Planspiele und sog. „Minigames" aus den mehrfach ausgezeichneten Lernstationsformaten „SECURITY PARCOURS" bzw. „Security Arena" sowie generische Simulationen und Edutainment-Tools aus den zahlreichen Kampagnen von known_sense-Kunden verhindern eine rein theoretische Annäherung, sondern befähigen vielmehr zum Einüben und zur sofortigen Umsetzung. Damit folgen wir unserer Überzeugung, dass bei der Auseinandersetzung mit wichtigen Sicherheitsthemen lediglich ein hohes Involvement (und sogar Spaß!), ein persönlicher Sinn sowie individueller Nutzen notwendig sind. Das Erleben und das eigene Tätigwerden führen zu einer dauerhaften und nachhaltigen Verhaltensänderung – und damit zu mehr Sicherheit – stets dem (diskursiven) Prinzip „Talking Security" folgend, dem Sprechen über Sicherheit & Co.

Wie viel Zeit muss ich einplanen?

Wir bieten WorkOuts in verschiedenen „Trainingsstärken" – alle lassen sich modular verbinden, so dass die vielfältigen Themen in verschiedenen Intensitäten vorgestellt und eingeübt werden können, je nachdem was notwendig ist. So lassen sich die WorkOuts leichter kombinieren, ggf. in geplante Awareness-Maßnahmen einbetten und in den Arbeitsalltag integrieren. Sie können wählen zwischen:

- **ImpulsWorkout** – 2–3 Stunden
- **MediumWorkout** – halbtägiges Training von 4 Stunden
- **IntensivWorkout** – ganztägige Veranstaltung von 8 Stunden
- **WorkoutEvent** (z. B. die „Security Arena") skalierbar von 1 Stunde bis zu mehreren aufeinander folgenden Tagen

Wie viele Personen können an den WorkOuts bzw. Events teilnehmen?

Wir bieten WorkOuts von 2 bis ca. 30 Personen pro Veranstaltung an. Bei Impuls- oder MediumWorkouts können 2-4 Workouts an einem Tag stattfinden. Events wie die „Security Arena" sind von 1 Stunde bis auf mehrere Tage hintereinander mit etwa 10 bis täglich 250 Teilnehmer skalierbar.

Wo finden die WorksOuts statt?

Normalerweise bieten wir unser WorkOuts als Inhouse-Schulungen in Ihren Räumen an. Dabei sind wir nicht wählerisch und nehmen gerne, was Sie uns anbieten. Für Events wie die „Security Arena" gilt „Visibility VOR ruhig gestellter Rückzug", d. h. eine Arena sollte in meinem Unternehmen stets dort stattfinden, wo sich viele Kollegen aufhalten, damit Sichtbarkeit erzeugt wird – idealerweise in stark frequentierten Eingangsbereichen. Falls Sie keine geeignet Lokationen stellen können, kümmern wir uns selbstverständlich gerne um passende Räume.

Im Fokus unserer WorkOuts stehen Themen der klassischen Informationssicherheit, Cyber Security, Datenschutz, Compliance, Awareness und ihrer benachbarten Disziplinen:

Neben den wichtigen Themen zur Informationssicherheit befassen wir uns zunehmend mit digitaler Transformation und personeller Sicherheit. So beklagen viele Arbeitnehmer eine immer stärker werdende Gewalt am Arbeitsplatz und in den sozialen Netzwerken: Verrohung von Sitten sowie Bedrohungen, aber auch die Gefahr von Übergriffen psychisch labiler, überforderter Kunden und auch von Kolleginnen und Kollegen nehmen an Häufigkeit zu. Auch hierzu bieten wir ein WorkOut an mit dem Titel:

Aktuell in Planung sind weitere Security WorkOuts, z. B.:

- Security Casino – Entwicklung und Einsatz von Awareness-Plan- und Edutainment-Spielen
- Security NowHere – Sicherheitskultur im Unternehmen identifizieren und modellieren
- Security on the Go – sicher unterwegs
- Sicher informieren – Basis-WorkOut Datenschutz und Informationssicherheit
- Außerdem u. a. zu: den Themen Clear Desk, Informationsklassifizierung, Passwort, Apps & Co. sowie Security Incident Management, Reporting & Co.

Die Preise unserer Security-WorkOuts

In den Preisen sind jeweils inbegriffen: Standard-Vorbereitungen, Materialien, Handouts. Alle Teilnehmer erhalten im Anschluss an das Security-WorkOut ein digitales Fotoprotokoll. Je nach Teilnehmergröße und Dauer der Veranstaltung werden die Security-WorkOuts von einem oder zwei Trainern durchgeführt (außer bei „Sexy Security", „Security Arena" und „Security Spot" (s. Details und ggf. abweichende Trainerzahl bzw. Preise dort).

- **ImpulsWorkout** (2–3 Stunden) – ab 600,00 € zzgl. 19 % Mehrwertsteuer
- **MediumWorkout** (4 Stunden) – ab 1.000,00 € zzgl. 19 % Mehrwertsteuer
- **IntensivWorkout** (8 Stunden) – ab 1.500,00 € zzgl. 19 % Mehrwertsteuer

Hinzu kommen noch Reisekosten, (DB-Ticket, 2. Klasse oder KFZ mit 0,30 €/km) und ggf. Übernachtungskosten. Optionale, detaillierte Vor- und Nachbereitungen wie z. B. schriftliche Dokumentationen, Reports oder Konzepte werden extra abgerechnet.

Weitere Informationen: http://www.known-sense.de/2017_known_sense_Awarenessflyer.pdf

Haben Sie Fragen zu den Preisen oder möglichen Rabatten? Melden Sie sich bitte bei uns:

known_sense | Jakob-Engels-Straße 39 | 51143 Köln
Fon +49 2203 1831618 (Ansprechpartner Dietmar Pokoyski)
E-Mail und Web: sense@known-sense.de bzw. www.known-sense.de

INVOLVEMENT, SPASS, EIN PERSÖNLICHER SINN SOWIE INDIVIDUELLER NUTZEN – DAS ERLEBEN UND DAS EIGENE TÄTIGWERDEN FÜHREN ZU EINER DAUERHAFTEN UND NACHHALTIGEN VERHALTENSÄNDERUNG UND DAMIT ZU MEHR SICHERHEIT.

WIE IMMER GREIFEN WIR AUCH IN DEN WORKOUTS DIE SPEZIFISCHEN WIDERSPRÜCHE UND WIDERSTÄNDE IN BEZUG AUF DIE EINZELNEN THEMEN AUF – EBEN DIE PSYCHOLOGISCHE SEITE DER SICHERHEIT.

Hey, (hier der Boss) ich brauch' mehr Geld – Strategien gegen CEO-Fraud

Zielgruppe(n)	▸▸ Zielgruppen für CEO-Fraud – in der Regel Vorstände, (C-Level) Manager oder Personen mit vergleichbaren Rollen oder Rechten
Content (Auswahl)	▸▸ Social Engineering und Führungskultur – eigene Rolle und sozlale Verantwortung ▸▸ Ablauf von CEO-Fraud, d. h. Methoden der Trickbetrüger ▸▸ Aktuelle Zahlen und Erkenntnisse zu den verschiedenen Formen und Vorbereitungen des CEO-Fraud ▸▸ Vorgehensweisen der Betrüger hautnah erleben (Spear Phishing, Executive Whaling, Social Engineering & Co.) ▸▸ Psychologische Tricks und eigene Reaktionen wahrnehmen ▸▸ Screening der eigenen (sozialen) Schwachstellen ▸▸ Einfluss der Unternehmens- und Sicherheitskultur erkennen und geeignete Abwehrstrategien benennen und planen ▸▸ Trainieren individueller, kontextbezogener Fraud-Abwehr
Optionaler Medien-einsatz	▸▸ Tiefenpsychologische Studie „Hey, (hier der Boss) Ich brauch' mehr Geld" ▸▸ Selbsttest „Bluff-O-Meter" für Führungskräfte ▸▸ SE-Video und -Podcast ▸▸ Diverse SE-Planspiele, u. a. Security Arena-Minigames („Phishing", „CEO-Fraud" und „Social Media – Fake Profile")
Ziele (Auswahl)	▸▸ Manager als Sicherheitsvorbilder und „Last Line of Fraud-Defense" ▸▸ Kenntnisse über Vorgehen von Trickbetrügern ▸▸ Erkennen und Benennen von Sicherheitskultur, Schwachstellen im eigenen Unternehmen und individueller Einfalltore ▸▸ Planen und Trainieren von Awareness- und Defense-Strategien ▸▸ Sensibilisierung für Hinweise – Social Engineering Incident Management (Hinweisgebersysteme und lernende Auswertung)

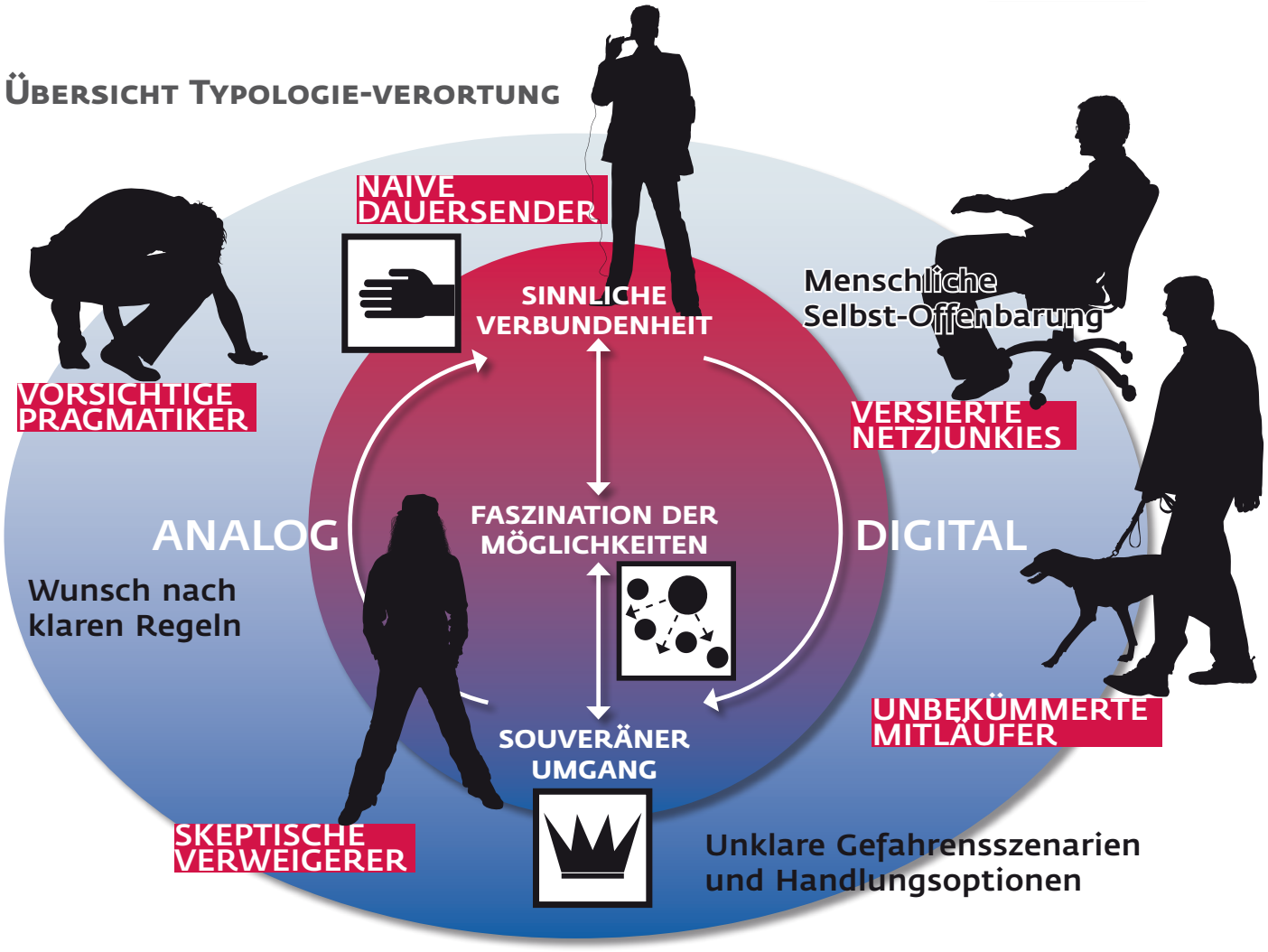
SOCIAL ENGINEERING

Bluff me, please – Social Engineering und falsche Identitäten

Zielgruppe(n)	⏩ Alle Mitarbeiter, insbesondere solche mit zahlreichen Außenkontakten (Management, Chefsekretariate, Empfänge etc.)
Content (Auswahl)	⏩ Was ist bzw. warum und wie gut funktioniert Social Engineering? ⏩ Möglichkeiten und (weitere) Formen der Manipulation (CEO-Fraud, Phishing, Desinformation & Co.) ⏩ Einfluss der Fehler- und Sicherheitskultur auf Social Engineering & Co. ⏩ Soziale Einfalltore – Grundlagen menschlicher Kommunikation, Kommunikationsebenen – analog und digital ⏩ Grundlagen des menschlichen Miteinanders: soziale Eigenschaften – Stärken und Schwächen ⏩ Social Engineering Incident Management und Reporting, Scham
Optionaler Medien-einsatz	⏩ Tiefenpsychologische Studie „Bluff me, if U can" ⏩ Selbsttest „Bluff-O-Meter" ⏩ SE-Video und -Podcast ⏩ SE-Planspiele, u. a. „Bluff & Hack" ⏩ Diverse Security Arena-Minigames („Phishing", „Social Engineering", „Social Media – Fake News")

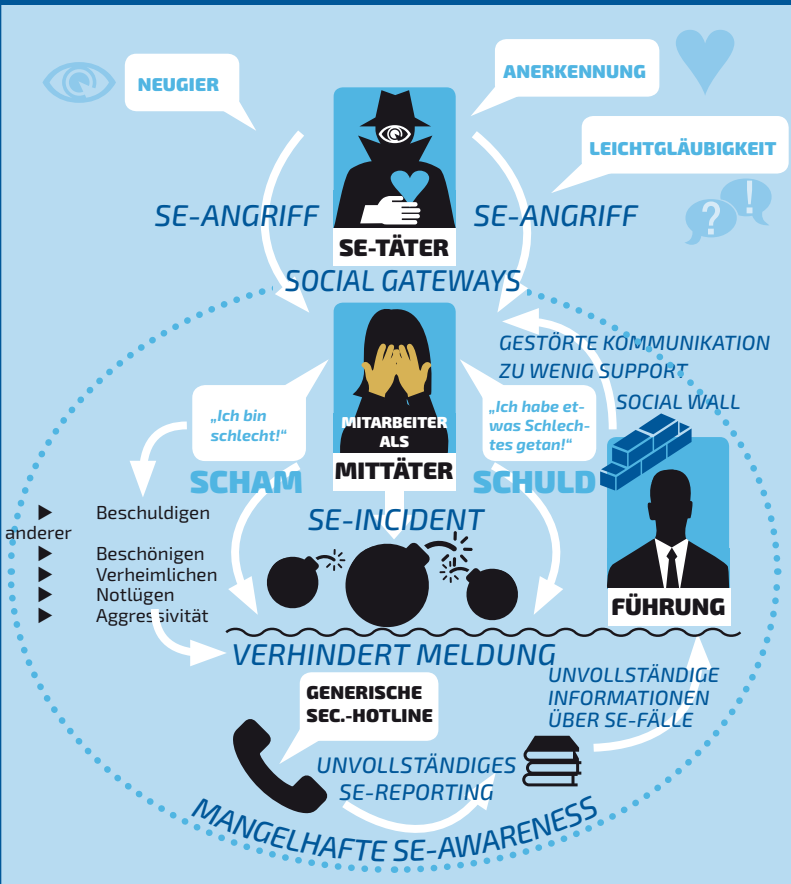
Ziele (Auswahl)	⏩ Was bedeutet Social Engineering, warum gibt es so etwas und wie erkenne ich das?
	⏩ Bewusstsein schaffen für Methoden und Ziele des Social Engineerings sowie die (Defense-)Möglichkeiten jedes einzelnen Mitabeitenden
	⏩ Erkenne dich selbst:
	  ⏩ Analyse des eigenen Kommunikationsverhaltens
	  ⏩ Analyse der individuellen Einfalltore für Social Engineering
	⏩ Einüben individueller Kommunikationstechniken
	⏩ Erarbeiten kontextbezogener und individueller Abwehrstrategien (Defense-Maßnahmen) im Rahmen der alltäglichen Kommunikation

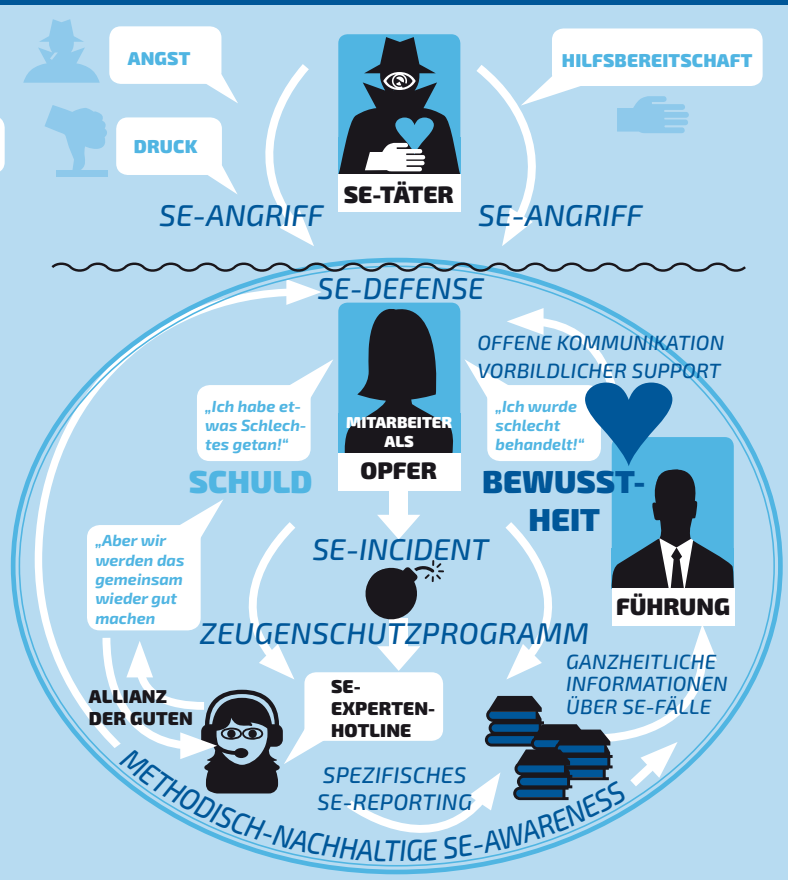
Übersicht Typologie-Verortung



„Ich bin der Fehler" – Schuld, Scham, Viktimisierung bei Social Engineering

Mitarbeiter als Mittäter (Abb. l.) vs. Mitarbeiter als Opfer bzw. Zeuge (Abb. r.)





Von der Ente zur End-Täuschung – Desinformation und alternative Wahrheiten

Zielgruppe(n)	▸▸ Alle Mitarbeiter, die Desinformationen vermeiden wollen, insbesondere aus den Kommunikations- und Sicherheitsbereichen
Content (Auswahl)	▸▸ Formen der Desinformationen und Unterschiede von Desinformation – je nach Relevanz der Information ▸▸ Möglichkeiten und Formen von Manipulation, Social Bots & Co. ▸▸ Rolle und Einflüsse der verschiedenen Informationskanäle ▸▸ Auswirkungen von Desinformation auf Unternehmen, Unternehmens- und Sicherheitskultur ▸▸ Psychologische Aspekte der Desinformation ▸▸ Individueller Umgang mit Informationen und Meinungen ▸▸ Möglichkeiten zur Überprüfung bzw. Verifizierung von Informationen
Optionaler Medien-einsatz	▸▸ Tiefenpsychologische Studie „Von der Ente zur End-Täuschung" ▸▸ Selbsttest „Influene-O-Mat" ▸▸ Security Arena-Minigame „Fake News"
Ziele (Auswahl)	▸▸ Erkennen von Falschinformationen und konkretes Vorgehen bei Überprüfung von Quellen ▸▸ Aufbau von individuellen Informations- und Abwehrstrategien bei Fake ▸▸ Gekonntes Handlungsrepertoire zur Überprüfung von Informationen und geeignetem Handeln entwickeln und einüben

SOCIAL MEDIA

Social Media Profi oder Media Zombie? Sicher ‚pröffentlich' in Networks	
Zielgruppe(n)	▸▸ Alle Mitarbeiter, die beruflich und privat soziale Medien nutzen ▸▸ Optional (tiefenpsychologischer) Fokus für Kommunikationsprofis ▸▸ Optional für Eltern private Nutzung durch Kinder bzw. Familie

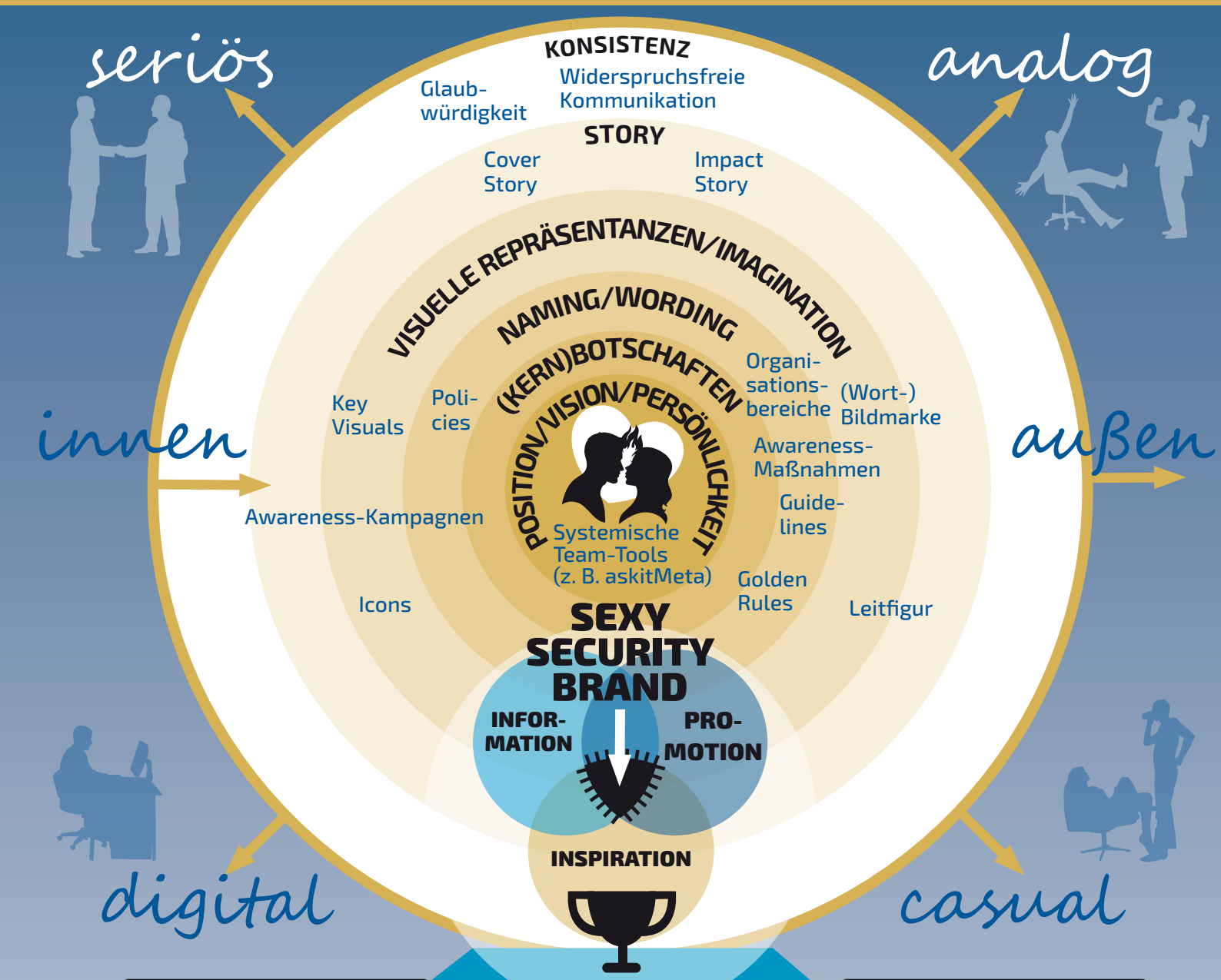
Content (Auswahl)	▸▸ Wo und wie bewegen wir uns in den sozialen Medien, welche digitalen Fußspuren hinterlassen wir?
	▸▸ Risiken: Fraud, Social Engineering, Social Bots, Fake Profile, Shit Storm, Cyber Mobbing, Grooming & Co.
	  ▸▸ Sicherheitsaspekte der einzelnen Medien
	  ▸▸ Hinweise auf mögliche ‚Nutzung' der eigenen Daten im Hinblick auf Social Engineering, Fraud & Co.
	▸▸ Veränderungen des Kommunikationsverhaltens und der Beziehungsgestaltung im Arbeitsumfeld durch Einsatz von Social Media & Co.
	▸▸ Den eigenen Status der ‚Pröffentlichkeit' erkennen und Grenzen zwischen privat und öffentlich definieren
	▸▸ Getriebener der sozialen Medien? – Offline-Möglichkeiten sozialer Kontakte

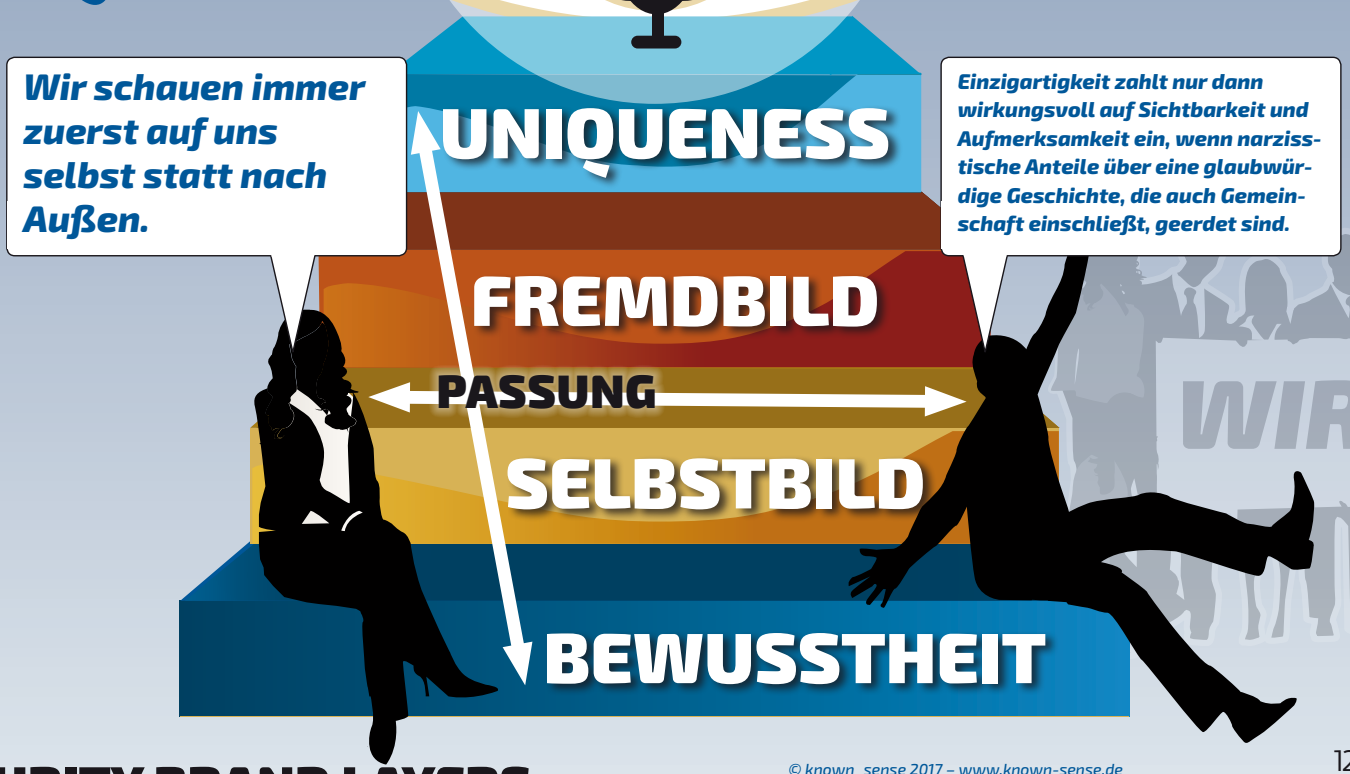
Optionaler Medien-einsatz	▸▸ Diverse Social-Media-Planspiele, u. a. Security Arena-Minigames („Social Media" und „Social Media – Fake Profile")
Ziele (Auswahl)	▸▸ Differenzierter Umgang mit sozialen Medien ▸▸ Vorteile und mögliche Risiken einzelner Medien bewusst erkennen und kompetent agieren ▸▸ Gestaltung der Arbeits- und Sicherheitskultur durch Nutzung von Social Media ▸▸ Sozialen Medien und Compliance-Richtlinien bzw. Social Media-Guidelines des Arbeitgebers in Einklang bringen ▸▸ Für Kommunikationsprofis: Social Media Guidelines richtig worden und gestalten

Sexy Security: Sicherheit als Marke – Aufbau, Positionierung und Pflege

Zielgruppe(n)	▸▸ Alle, die am Aufbau von Security als Marke beteiligt sind: CISO & Co., Security Manager und -experten, Privacy und Compliance Officers, HR- und Change Manager, Kommunikationsexperten, Trainer u. v. m.
Content (Auswahl)	▸▸ Wie positioniere ich Security auf eine attraktive Art und Weise? ▸▸ Grundlagen von Security Branding und Positionierung von Security-Protagonisten, Team, Security-Kommunikationsstil und -Maßnahmen ▸▸ Lobbyarbeit: Positionierung von Security (Unternehmen, Führung etc.) ▸▸ Anwendung von Kommunikationstools (z. B. „askitMeta", „Security Spot") ▸▸ Naming, Branding, Leitfiguren, Key Visuals Story Telling – was gehört zu einer gelungene Ansprache und wie finde ich einen passenden Stil? ▸▸ Gamification – Spieleprinzipien, – wirkungen und -Design ▸▸ Inhouse-Kreativität oder Steuerung externer Partner (z. B. Agenturen)
Optionaler Medien-einsatz	▸▸ Verschiedene tiefenpsychologische Security Studien ▸▸ Verschiedene Gamification bzw. weitere Good Practice Tools (Logos, Leitfiguren, Key Visuals, Awareness Edutainment, Videos u. v. m.) ▸▸ Diverse Checklisten
Ziele (Auswahl)	▸▸ Entwicklung von Sicherheit, seiner Bereiche, Protagonisten und Maßnahmen als Marke inklusive Sichtbarkeit, Story bzw. Sinn ▸▸ Findung von passenden Stellvertretern für Sicherheit und Detailaspekte (Kreativität auf Knopfdruck, Wording, Naming, Imagination?) ▸▸ Planung von begeisternden Maßnahmen bzw. kompletter Kampagnen ▸▸ Passgenau auf die Unternehmenskultur ausgerichtet ▸▸ Story Telling und Involvement durch Sinn-Haftigkeit inklusive ▸▸ Zielgruppenspezifische Themen und passgenaue Ansprache ▸▸ Nachhaltig und wirksame Steigerung der Sichtbarkeit von Security
Optionen	▸▸ „SEXY SECURITY" ist eine Marke unserer TAKE AWARE EVENTS Optional ist diese Veranstaltung – wie auch der gleichnamige Kongress – mit mehr als einem Trainer duchführbar, d.h. Experten aus den o. g. Bereichen können optional hinzugebucht werden ▸▸ Damit ist die Teilnehmerzahl aufgrund paralleler Streams skalierbar

SECURIBILITY – AUF WELCHEN LAYERN WIRKT SICHERHEITS-KOMMUNIKATION?





SECURITY BRAND LAYERS

AWARENRESS-STRATEGIE

Awareness you can touch – Awareness-Planungs-Workshop mit askitMeta

Zielgruppe(n)	▸▸ Mitarbeiter, die am Aufbau von Security Awareness beteiligt sind: CiSO & Co., Awareness-Manager und -experten, Privacy und Compliance Officers, HR- und Change Manager

Content (Auswahl)	▸▸ Grundlagen gelungener Awareness und Bedeutung für die Kampagnenplanung, z. B.:
	  ▸▸ Gewinnung von Stakeholdern, Bilden einer zentralen Planungsmannschaft (Security-Core-Team)
	  ▸▸ Awareness-Lobbying bzw. Positionierung des Themas im Unternehmen
	▸▸ Themen, Zielgruppen- und Verfassungs-Marketing
	▸▸ Bilder, Themen, Zielgruppen Kanäle identifizieren via Planspiel askitMeta
	▸▸ Naming, Branding, Leitfiguren, Story Telling – was gehört zu einer gelungene Ansprache?
	▸▸ Gamifikation – Möglichkeiten und Vorteile involvierender Maßnahmen kennenlernen und ausprobieren
	▸▸ Steuerung von Inhouse-Teams und Dienstleistern, insbesondere Agenturen
	▸▸ Dokumentation bzw. Erfolgsevaluation

Optionaler Medien-einsatz	▸▸ Verschiedene tiefenpsychologische Security Studien ▸▸ Verschiedene Good Practice Tools (Leitfiguren, Key Visuals, Planspiel, Awareness Edutainment-Tools, Videos u.v.m. ▸▸ Checklisten

Ziele (Auswahl)	▸▸ Entwicklung einer Awareness-Strategie bzw. eigener Awareness-Tools
	▸▸ Planung einer begeisternden Awareness-Kampagne
	  ▸▸ Passgenau auf die Unternehmenskultur und Zielgruppen bzw. Verfassungen ausgerichtet
	  ▸▸ Zielgruppenspezifische Ansprache und Themen
	  ▸▸ Nachhaltig und wirksame Steigerung der Awareness
	  ▸▸ Success Stories und Visibility erzugen über Messbarkeit via quantitativer wie auch qualitativer Instrumente
	▸▸ Austausch, Feedback und Supervision eigener Kampagnen-Ideen
	▸▸ **Einfache Workshop-Dokumentation oder detailliertes Konzept bzw. Konzept-Challenging im Nachgang gegen Aufpreis**

MANAGEMENT AWARENESS

Security Spot – das Management Risk Asssessment & Awareness Game

Zielgruppe(n)	⏩ Vorstände, Management Boards, Führungskräfte
Content (Auswahl)	⏩ Management Risk Assessment (Cover Story) und Awareness-Workshop (Impact Story), um Security Teams und Management zu einem Austausch zu motivieren, Management Reviews zu implementieren sowie Risiken und weitere Security-Themen, die sich der herkömmlichen Prozesskommunikation weitgehend entziehen, zu bewerten und zu visualisieren ⏩ Material: askitMeta-Moderationskarten zzgl. Spielfeld mit individuell ausgefülltem Business Framework, um zu visualisieren, in welchen konkreten Geschäftsfeldern die priorisierten Risiken Wirkung entfalten
Optionaler Medien-einsatz	⏩ Pre-Workshop mit Security Professionals, um ein Business Framework zu erstellen ⏩ Post-Begleitung der Auswertung (wahlweise als einfache Dokumentation oder als detaillierten Report) sowie Post-Präsentation vor dem Management gegen Aufpreis
Ziele (Auswahl)	⏩ Priorisierung bei der Identifikation von Risiken ⏩ Übernahme von Sponsorships für Risiken und ihrer Defense-Maßnahmen. ⏩ Erstellung einer Entscheidungsvorlage, basierend auf den Top-5-Risiko-Priorisierungen ⏩ Erstellung von Report und Maßnahmenkatalog (gegen Aufpreis) ⏩ Klärung von Rollen und Positionen im Kontext von Sicherheit bzw. Sicherheitskommunikation ⏩ Evaluation von Security Bedarfe ⏩ Steigerung der Security Awareness von Board Members ⏩ Mediation zwischen Security Professionals und Manager ⏩ Kreation von lebendigen Security Lernkarten ⏩ Bildung von Security- und Awareness-Arbeitsgruppen ⏩ **Pre-Workshop, Dokumentation, Report und weitere Begleitung gegen Aufpreis. Detaillierte Informationen im Security Spot-Flyer**

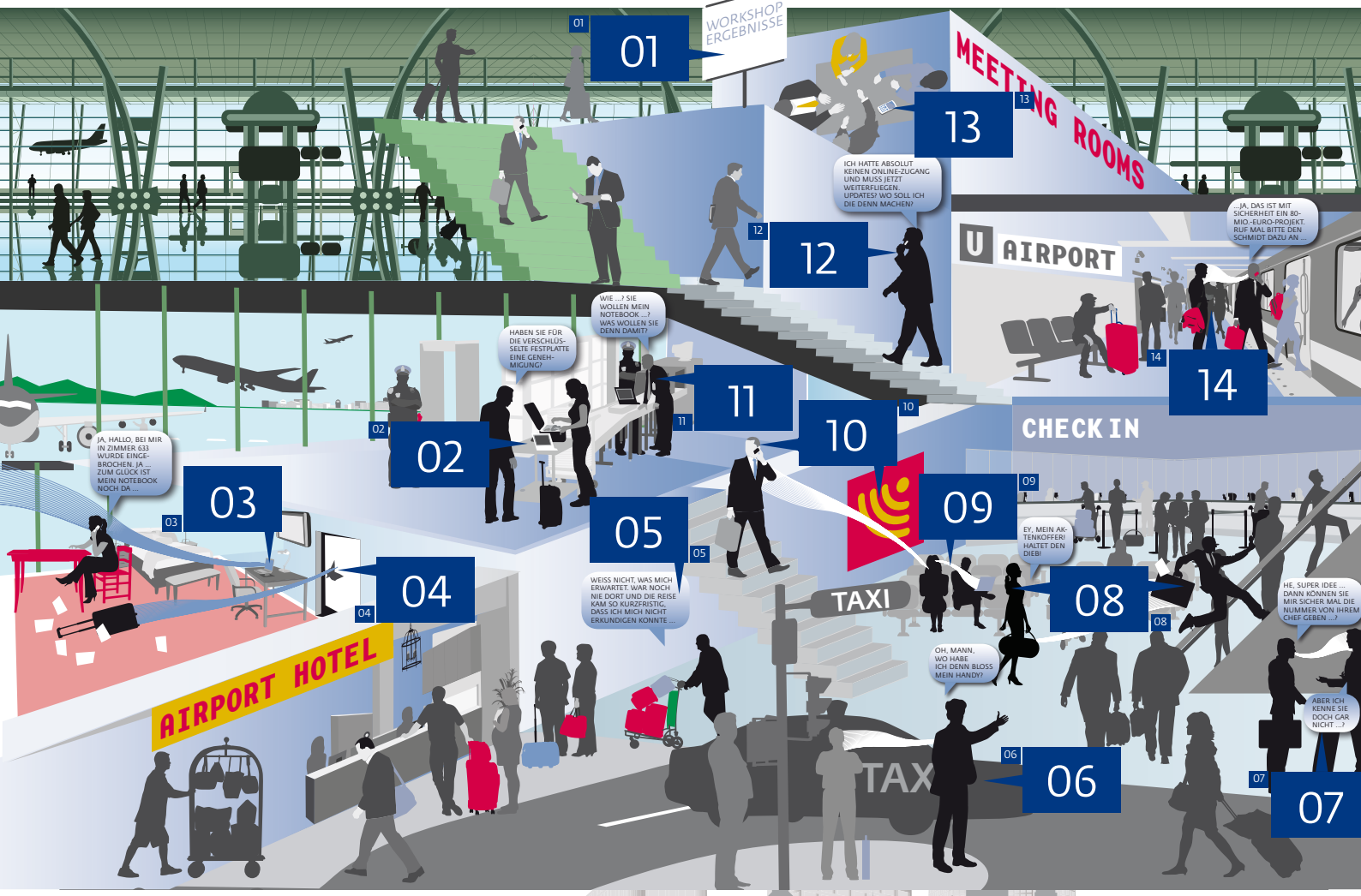
LERNSTATION-ROADSHOW

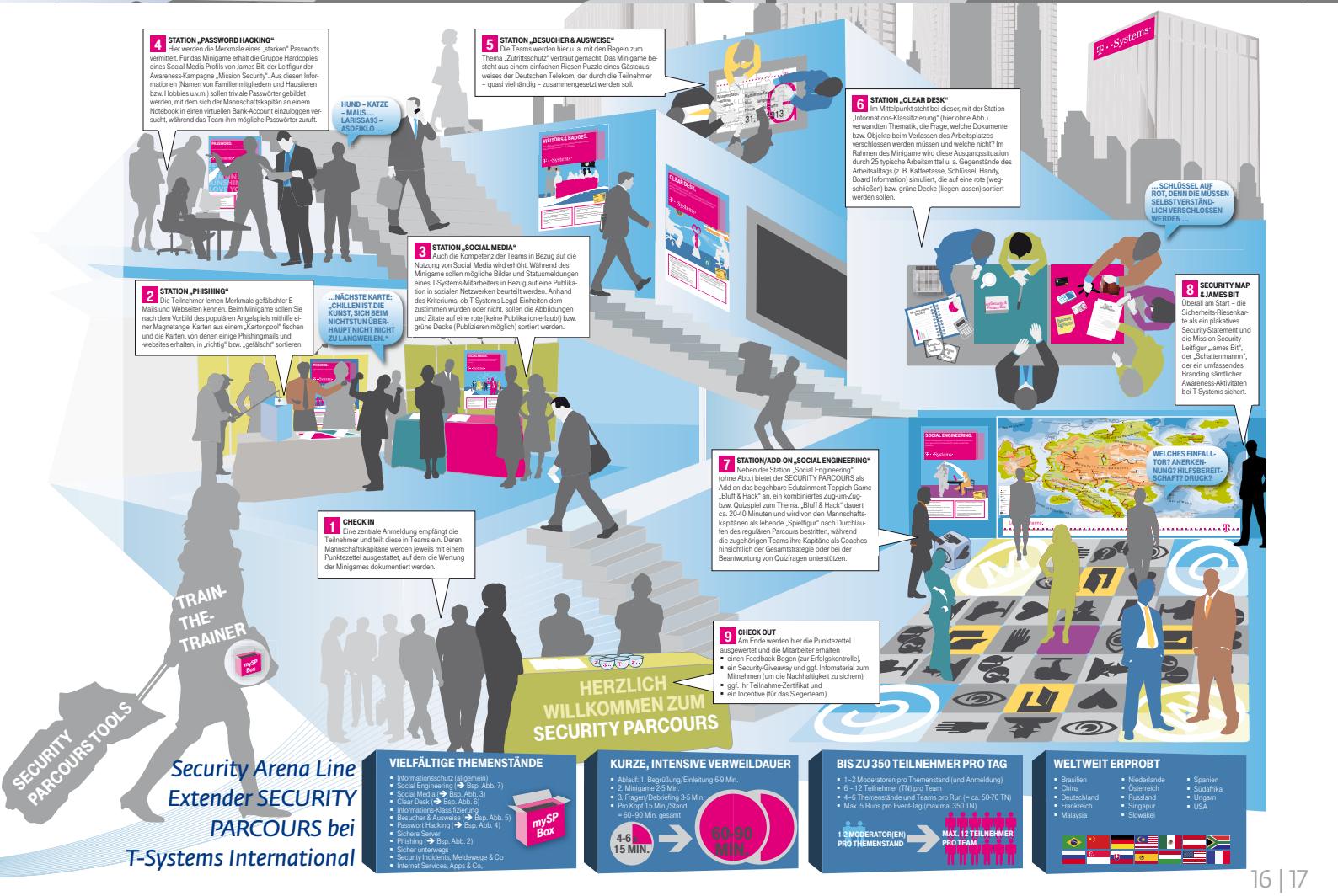
Security Arena – das Awareness Circle-Training ‚out of the box'

Zielgruppe(n)	▸▸ Alle Mitarbeiter, ▸▸ Spezifische Zielgruppen: Pacours für Manager, IT-Admins etc. möglich
Content (Auswahl)	▸▸ Verfügbare Stationen: Data Privacy, Social Engineering (jew. 2 verschd. Games), Informationsklassifizierung, Clear Desk, Passwort Hacking, Sicher unterwegs, Phishing, Social Media, Social Media – Fake Profile, Besucher & Ausweise, Sichere Server, Incident Management, Reporting & Co., Apps, Web Services & Co., Cyber Security, Desinformation, Fake News & Co. – weitere in der Entwicklung ▸▸ Alles auf Deutsch/Englisch verfügbar – weitere Sprachen möglich ▸▸ Kunde sucht sich 4 oder 6 Stationen aus ▸▸ Incentivierung empfohlen (inkl. Preise für Siegerteam)
Optionaler Medien-einsatz	▸▸ Ausdehnung bzw. Verdichtung durch Event-Add-Ons wie Security. Marktplatz, World Café, begehbare Riesenspiele, Videos, Vorträge etc.
Ziele (Auswahl)	▸▸ Sicherheitsthemen werden durch den diskursiven Team-Ansatz in einen produktiven Umsatz gebracht ▸▸ Spielerischer Ansatz schafft hohes Invovement und verbindet Sicherheit mit positiven Erlebnissen (Emotion steigert Memorierbarkeit) ▸▸ Setting sichert hohe Visibility und adressiert die Intensivierung diverser Memo-Techniken ▸▸ Als Teaser für vertiefende Maßnahmen oder Kampagnen-Launch ▸▸ Gewinnung von Sicherheits-Vorbilder bzw. -Botschaftern

Teilnehmer-zahl, Preise & Optionen	▸▸ 1 Trainings-Run = 60 (4 Stationen) oder 90 Minuten (6 Stationen
	▸▸ Bis zu 6 Stationen pro Event-Tag möglich mit z. B.
	  ▸▸ bis 20 TN ab 600,00 Euro netto zzgl. Reisekosten
	  ▸▸ bis 35 TN ab 1.000,00 Euro netto zzgl. Reisekosten
	  ▸▸ bis 70 TN ab 1.500,00 Euro netto zzgl. Reisekosten
	  ▸▸ bis 140 TN ab 2.800 Euro netto zzgl. Reisekosten
	  ▸▸ bis 280 TN ab 4.800 Euro netto zzgl. Reisekosten
	▸▸ **Alle Materialien können auch lizenziert und über unseren Train-the-trainer-Ansatz eigenständig in Organisationen implementiert werden. Detaillierte Infos** www.known-sense.de/SecurityArena.pdf

SICHER UNTERWEGS





Security Arena Line Extender SECURITY PARCOURS bei T-Systems International

VIELFÄLTIGE THEMENSTÄNDE
- Informationsschutz (allgemein)
- Social Engineering (→ Bsp. Abb. 7)
- Social Media (→ Bsp. Abb. 3)
- Clear Desk (→ Bsp. Abb. 6)
- Informations-Klassifizierung
- Besucher & Ausweise (→ Bsp. Abb. 5)
- Passwort Hacking (→ Bsp. Abb. 4)
- Sichere Server
- Phishing (→ Bsp. Abb. 2)
- Sicher unterwegs
- Security Incidents, Meldewege & Co
- Internet Services, Apps & Co.

mySP Box

KURZE, INTENSIVE VERWEILDAUER
- Ablauf: 1. Begrüßung/Einleitung 6-9 Min.
- 2. Minigame 2-5 Min.
- 3. Fragen/Debriefing 3-5 Min.
- Pro Kopf 15 Min./Stand = 60-90 Min. gesamt

4-6 15 MIN. → 60-90 MIN.

BIS ZU 350 TEILNEHMER PRO TAG
- 1–2 Moderatoren pro Themenstand (und Anmeldung)
- 6 – 12 Teilnehmer (TN) pro Team
- 4–6 Themenstände und Teams pro Run (= ca. 50-70 TN)
- Max. 5 Runs pro Event-Tag (maximal 350 TN)

1-2 MODERATOR(EN) PRO THEMENSTAND → MAX. 12 TEILNEHMER PRO TEAM

WELTWEIT ERPROBT
- Brasilien
- China
- Deutschland
- Frankreich
- Malaysia
- Niederlande
- Österreich
- Russland
- Singapur
- Slowakei
- Spanien
- Südafrika
- Ungarn
- USA

PERSONELLE SICHERHEIT

Safety First – personelle Sicherheit in unsicheren Zeiten

Zielgruppe(n)	⏩ Alle Mitarbeiter, die beruflich Konflikten und Gewalt ausgesetzt sein können – auf der Arbeit bzw. den Wegen von und zur Arbeit, beim Einkauf, z. B. im Einkaufszentrum, in der Gastronomie, bei, vor und nach Veranstaltungen u. a. Events bzw. generell in der Öffentlichkeit
Content (Auswahl)	⏩ Themen u. a. Amok, Terror, (Cyber) Mobbing, Stalking und allgemein angstfreies Arbeiten ⏩ Sensibilisierung für das Thema Gewalt – vor der Gewalt ⏩⏩ Klärung: Wann ist etwas Gewalt, wer entscheidet darüber? ⏩⏩ Sensibilisierung für Situationen und Signale ⏩ Techniken während der Situation: ⏩⏩ Deeskalationsstrategien: Kommunikation und Körpersprache beherrschen – trotz Stress! ⏩⏩ Handlungsoptionen zur Konfliktminderung und Konfliktlösung kennen und einüben ⏩ Nach dem Ereignis ⏩⏩ Psychische Reaktionen nach Gewalt und Unsicherheit ⏩⏩ Was können Kollegen, Vorgesetze, Betroffene tun?
Optionaler Medien-einsatz	⏩ Verschiedene Übungssequenzen ⏩ u. a. Security Arena-Minigame „Amok & Terror"
Ziele (Auswahl)	⏩ Erkennen von Gefahrenindikatoren, Justieren des persönliches Gefahrenradars ⏩ Anwenden von Deeskalationsstrategien ⏩ Beherrschen von Handlungsoptionen zur Konfliktminderung und Konfliktlösung ⏩ Vermeiden von psychischen Langzeitfolgen
Optionen	⏩ Skalierbar durch Inhalte bzw. weitere Trainer resp. Referenten des von uns mitorganisierten Kongresses „FEARLESS"

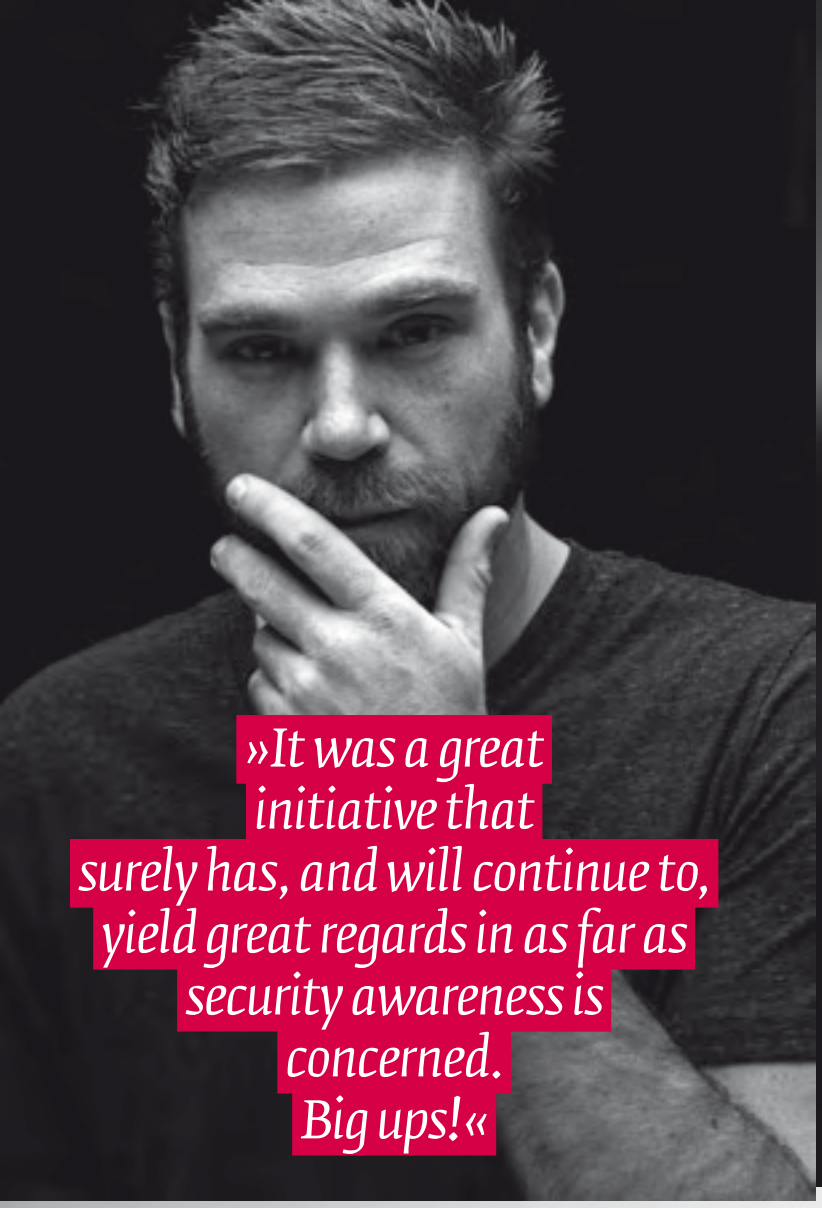
Yes, we cyber – sicher durch die Digitalisierung

Zielgruppe(n)	▸▸ Alle Mitarbeiter, die bereits Erfahrungen mit der digitalen Transformation gesammelt haben oder unmittelbar vor dem Transformationsprozess stehen – auch Führungskräfte mit Personalverantwortung
Content (Auswahl)	▸▸ Klärung von Begrifflichkeiten: digitale Diktatur oder digitale Evolution? Was macht Digitalisierung aus? Was bedeutet Arbeitswelt 4.0 konkret für das eigene Unternehmen? ▸▸ Barrieren und (emotionale) Widerstände der Digitalisierung identifizieren: Überforderung, Sorge vor Arbeitsplatzverlust etc. ▸▸ Chancen und Potenzial der digitalen Veränderungen: Verbesserung von Arbeitsprozessen, (persönliches) Wachstum etc. ▸▸ Relevante Bereiche der Digitalisierung feststellen, z. B. digitale Daten, Automatisierung, digitaler Kundenzugang, Vernetzung ▸▸ Veränderungen der Kommunikation durch digitale Transformation ▸▸ Aspekte der (informations-)Sicherheit und des Datenschutzes: digital und sicher – wie geht das, wer ist dafür verantwortlich?
Optionaler Medien-einsatz	▸▸ Visualisierungstechniken ▸▸ Neue Digitalisierungsstudie „Yes, we cyber“ ▸▸ Stationen des neuen „Digital-Parcours“ (z. B. „Future Jobs“, „Internet Services, Apps & Co.”, „Fake News“)
Ziele (Auswahl)	▸▸ Entwicklung geeigneter Schritte auf dem Weg zur digitalen Transformation, z. B. Kommunikationsstrategie ▸▸ Abbau von Barrieren gegenüber der digitalen Transformation ▸▸ Bewusstsein schaffen für die Risiken der digitalen Vernetzung ▸▸ **Einfache Workshop-Dokumentation oder detailliertes Konzept bzw. Konzept-Challenging im Nachgang gegen Aufpreis**

»Well presented. Trainers were warm, smiling, make feel you at home, friendly.«

»I would recommend this to all employees, so make it compulsory to attend.«

»I feel it's easier to learn when having fun, and this event provided exactly that.«



»It was a great initiative that surely has, and will continue to, yield great regards in as far as security awareness is concerned. Big ups!«

»Danke für diesen super Tag.«

»The event was very educational, fun, and challenging as it required us to think and act urgently, with caution and working with a group of individuals who are unique. It was wonderful.«

known_sense – Dozenten und Trainer mit dem Blick hinter die Kulissen

Alle WorkOuts werden von tiefenpsychologisch ausgebildeten Trainern durchgeführt. Wir verfügen über jahrelange Erfahrung, haben zahlreiche qualitative Sicherheits-Studien zu verschiedenen Security Topics sowie Awareness-Kampagnen in mehr als 50 bzw. Awareness-Trainings und -Events in 30 Ländern auf 5 Kontinenten durchgeführt – außerhalb Europas u. a. in Australien, Malaysia, Singapur, Thailand, Südafrika, Brasilen, Mexiko bzw. den USA. Darauf basierend bieten wir sämtliche WorkOuts nicht nur auf Deutsch, sondern auch auf Englisch an.

Ankha Haucke ist Diplom Psychologin und Therapeutin mit eigener Praxis für Einzel- und Paartherapie in Köln. Bei known_sense ist sie u. a. für Trainings sowie für Konzeption und Feldarbeit von tiefenpsychologischen Security-Wirkungsanalysen verantwortlich Darüber hinaus ist sie Co-Autorin des psychologischen Fachbuchteils von „Security Awareness", erschienen bei Vieweg Springer.

Ivona Matas ist Diplom-Psychologin, Therapeutin, qualitative Marktforscherin und verfügt über eine Train-the-Trainer-Ausbildung. Bei known_sense ist sie u. a. verantwortlich für die Durchführung von tiefenpsychologischen Security-Wirkungsanalysen, Begleitung von Kampagnen mithilfe qualitativer Wirkungsforschung sowie Führungskräfte-Entwicklung. Sie führt Präsenztrainings und Social-Engineering-Maßnahmen durch. Unsere Angebote zur personellen Sicherheit profitieren von ihrer langjährigen Erfahrung auf den Gebieten Notfallpsychologie und Maßnahmen zum Erhalt der psychischen Gesundheit in Unternehmen.

Dietmar Pokoyski, Mitveranstalter der TAKE AWARE EVENTS mit der weltweit einzigen reinen Social-Engineering-Konferenz BLUFF CITY, ist Geschäftsführer der Awareness-Agentur known_sense und gemeinsam mit Michael Helisch Autor des einzigen Fachbuchs zum Thema in Deutschland. Seit 2005 hat er Awareness-Kampagnen und als Trainer und Supervisor Game Based Security Events in 60 Ländern und 30 Sprachen durchgeführt. Mit known_sense erhielt er zahlreiche Auszeichnungen, u. a. den „IT-Sicherheitspreis NRW" (2007) sowie den „OSPA – Oustanding Security Performance Award" (2015) für eine herausragende Initiative für Sicherheitsschulungen.

Wir arbeiten auch mit zahlreichen Gastdozenten und -moderatoren aus den Bereichen Informationssicherheit, Datenschutz, Kreation, visuelle Kommunikation, Branding, Wording, Naming u. v. m.

AWARENESS NEXT GENERATION – ERPROBTE PLANSPIELE UND „MINIGAMES“ VERHINDERN EINE REIN THEORETISCHE ANNÄHERUNG, SONDERN BEFÄHIGEN VIELMEHR ZUM EINÜBEN UND ZUR SOFORTIGEN UMSETZUNG.

SOCIAL ENGINEERING-WHEEL

DIE PRAKTISCHE „BLUFF-O-METER"-DREHSCHEIBE
SOCIAL GATEWAYS & EMOTIONALE DIMENSIONEN

known_sense
awareness you can touch.