

S ex y

S ec u r i t y

»Sexy Security?«

Informationssicherheit aus Sicht der Tiefenpsychologie

Dietmar Pokoyski (known_sense)
eco AK Sicherheit/Köln, 03. Februar 2010

known_sense

- 2002ff. in Köln
- Kommunikationsagentur & Consulting
- Interne Komm., Employee Branding, (Security) Awareness, Kreation, Forschung
- 2007 IT-Sicherheitspreis NRW
- 2008 Gründungsmitglied aware-house

known_sense/Kunden

■ Klassisch

- Caritasverband für die Stadt Köln e.V.
- Cartamundi NV (Turnhout, Belgien)
- Citibank Privatkunden AG & Co. KgaA (Düsseldorf)
- Dokpop e.V. (Köln)
- Fahrzeug-Werke Lueg AG (Bochum)
- GiT – Gesellschaft für innovative DV –Techn. mbH (Gelsenkirchen)
- Heinrich-Heine-Institut (Düsseldorf)
- Institut der deutschen Wirtschaft Köln
- LAV-SOFO-MARKT (Stuttgart)
- Mattel GmbH (Dreieich)
- ORGA-SOFT Organisation und Software GmbH (Mainz)
- politikerscreen de AG (Berlin, heute: POLIXEA)
- rheingold (Köln)
- Spielkartenfabrik Altenburg GmbH
- Stadt Düsseldorf
- The Walt Disney Company (München)
- Wissenschaftszentrum Nordrhein-Westfalen (Düsseldorf)
- wiesmannforschenundberaten (Köln)
- wissenmedia GmbH (Gütersloh)

■ Security Awareness

- BIOTRONIK AG (Bülach, Schweiz)
- BIOTRONIK GmbH & Co. KG (Berlin)
- Cytec Industries Inc. (Wiesbaden/West Paterson, USA)
- Deutsche Telekom AG (Bonn)
- Dubai Municipality
- EnBW – Energie Baden Württemberg AG (Karlsruhe)
- IIR Technology GmbH (Sulzbach)
- ISPIN AG (Bassersdorf/Schweiz)
- Kanton Aargau (Aarau/Schweiz)
- M. DuMont Schauberg (Köln)
- Ringier AG (Zürich)
- ROLAND Rechtsschutz-Versicherungs-AG (Köln)
- Ruhr-Universität Bochum
- Stadt Ulm
- Sunrise Communications AG (Zürich)
- Schweizerische Mobiliar Versicherungsgesellschaft AG (Bern)
- T-Systems Enterprise Services GmbH (Bonn)
- Vattenfall Europe AG (Berlin)
- Vodafone D2 GmbH (Düsseldorf)
- WKÖ – Wirtschaftskammer Österreich (Wien)
- WSW Wuppertaler Stadtwerke GmbH

Wann ist
etwas
»sexy«?



Sexy? Sex Appeal?

- *appellare* (lat.) das ansprechen

Wann sind wir „angesprochen“?

- Wenn etwas uns berührt/bewegt.
- Wenn ein qualitativer Kontakt ermöglicht wird.
- Mensch will nicht mehr „Sex Appeal“, sondern mehr Liebe!

Sexy Security?

Wann ist Security „sexy“ Wann „spricht“ sie uns an?

- Wenn sie uns berührt/bewegt.
- Wenn sie einen qualitativen Kontakt ermöglicht.
- Mitarbeiter will nicht mehr Geld, sondern mehr Liebe (Anerkennung).

Grundproblem

Exkurs: Märchen ...

- ... sind komplexe Bilder der Wirklichkeit
- ... Vermitteln allgemeine menschliche Erfahrungen
- ... berühren, weil sie davon handeln, was uns im Innersten bewegt (z.B. Paradoxien)

**Auch wenn Menschen einzigartig sind,
teilen sie die Ur-Erfahrungen und die elementare Grundprobleme des Lebens!**

„Ver-rücktheiten“

- Leben gar **nicht so rational**, wie man das als aufgeklärter Mensch glauben mag
- Handlungen oft wider besseres Wissen
- Was auf ersten Blick **unverständlich**, macht oft **psychologisch Sinn** (z.B. geizige Reiche oder Menschen, die an Ihren Erfolgen scheitern)
- Brüche, Widersprüche, Unregelmäßigkeiten. „Verrücktheiten“, weil sich das Seelische **eindimensionalen Erklärungs-Kategorien** und Reiz-Reaktionsschemata widersetzt

Ja ist Ja – Nein ist Nein

- Grundprobleme unserer Kultur:

Paradoxe Verhältnisse werden abgespalten

- Nur das Rationale wird anerkannt
- Was wir sehen und zählen können,
- Was auf Knopfdruck an- und abgestellt werden kann

Gehirn-Pornos

- Bsp.: Aktueller Erfolg des Neuromarketings mit seinen Forschungs-Voyeurismus
 - es schwellen gewisse Zentren an
 - bestimmte Areale laufen rot an
 - es spritzen die Transmitter
- Henne-oder-Ei-Frage: Zeugt die bunte Spur in den Abbildungen dafür, dass Neurone psychische Effekte machen oder erzeugen die Gefühlszustände einen körperlichen Abdruck?

Paradoxes?

- Warum ist das Anerkennen von Paradoxem so schwer?
- Es braucht Zeit, bis sich etwas wandelt (Rückschritte, Stillstände, Zuspitzungen, etc.)
- s. Schleifen in Märchen (bis zu 7 mal) entspricht dem seelischen Entwicklungstempo

Grundproblem von Unternehmungen: keine Zeit für Schleifen und seelische Entwicklung

- „Objektive Wirklichkeit“ steht dem Nicht-Anerkennen von Paradoxem gegenüber

Unternehmenskultur?

- Problem von Unternehmenskulturen als Subkultur unserer Gesellschaft:

Es findet eine Zuspitzung des Grundproblems statt, z.B.

- Klassische Betriebswirtschaftslehre mit reiner Gewinnmaximierung
- Rein quantitative Denkweise
- Psychologie nur als verhaltensorientierte Disziplin, etc.

Sicherheitskultur?

Es findet wiederum eine Zuspitzung des Grundproblems von Unternehmenskultur statt:

- Alles wird „abgedichtet“
- Der Mensch wird zum Handlanger technologische und organisatorische Instrumente

Security befindet sich in der Isolation, ist „unsexy“!

- Widersprüche und Entwicklungen haben keinen Platz mehr

Security = Schwarzer Peter für MENSCHLICHE DEFIZITE in der (Unternehmens-)Kultur!

- „Die Geister, die man rief, wird man nicht wieder los!“

Sicherheit messen?

z.B. quantitative Verfahren

- Vorgefertigte Fragebögen sind für einen Zugang zum Seelenleben ungeeignet, da Kategorien des Erlebens bereits implizit vorgegeben mit geringem Gestaltungsraum
- Enthalten keine Widersprüche oder Übergänge
- Man mogelt und biegt sich Antworten zurecht, weil eigene Antworten nicht ins Schema passen
- Nachweisliches Messen von Wissen belegt keine Awareness!

z.B. Wirkungsanalysen

- Anders als konventionelle, quantitative Instrumente kein Teil der gesellschaftlichen Stilllegung
- WA benötigen nur wenige Tiefeninterviews (face-to-face, ca. 2 Stunden)
- Ziel: Sinn („geheime Logik“) verstehen
- Wirkungseinheiten und Verfassungen beschreiben
- Widersprüche, Übergänge, Zwischentöne sichtbar machen (und in Kommunikation übersetzen)

Best Practice Analysen

- Securitystudien





z.B.
Wirkungs
analysen

Wirkungsanalysen

- »Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen« (2006)
- Ziel: Klärung der verdeckten Motive s.g. **Mitarbeiter-Fehlleistungen**
- Korrigierte als Grundlagenstudie und erste tiefenpsychologische Securityforschung (klischeehafte) **Annahmen der IT-Sicherheit**



ANNAHME

z.B.
Wirkungs
analysen

Triviale Passwörter werden aus reiner Bequemlichkeit vergeben.

WIRKLICHKEIT?



ANNAHME

z.B.
Wirkungs-
analysen

Triviale Passwörter werden aus reiner Bequemlichkeit vergeben.

Über triviale Passwörter wird Persönliches in zunehmend entmenschlichte Unternehmenskultur transportiert.

WIRKLICHKEIT!



ANNAHME

z.B.
Wirkungs
analysen

Malware & Co. werden als zerstörerischer Angriff des eigenen Systems verstanden.

WIRKLICHKEIT?



ANNAHME

z.B.
Wirkungs
analysen

Malware & Co. werden als zerstörerischer Angriff des eigenen Systems verstanden.

Malware, Hacker u.a. Eindringlinge. üben ungeteilte Faszination aus, auf die Mitarbeiter geradezu sehnsüchtig warten.

WIRKLICHKEIT!



ANNAHME

z.B.
Wirkungs
analysen

Sicherheit soll nicht spürbar sein. Nur ein CISO, der ungesehen im Hintergrund operiert, ist ein „guter“ CISO.

WIRKLICHKEIT?



ANNAHME

z.B.
Wirkungs
analysen

Sicherheit soll nicht spürbar sein. Nur ein CISO, der ungesehen im Hintergrund operiert, ist ein „guter“ CISO.

Die Mitarbeiter wollen einen CISO als Marke – ein lebendiges Gesicht, Security als gute Story und in die Abwehr involviert werden.

WIRKLICHKEIT!



ANNAHME

z.B.
Wirkungs
analysen

Mitarbeiter-Fehlleistungen passieren aus Bequemlichkeit (oder, um sich zu rächen).

WIRKLICHKEIT?



ANNAHME

z.B.
Wirkungs
analysen

Mitarbeiter-Fehlleistungen passieren aus Bequemlichkeit (oder, um sich zu rächen).

Die Entsicherung am Arbeitsplatz dient einer Versicherung der eigenen Identität, weil sie über emotionale Faktoren die eigene Arbeitsfähigkeit im Unternehmen erhält.

WIRKLICHKEIT!



z.B.
Wirkungs
analysen

Zwischenfazit

- Die „Entsicherung am Arbeitsplatz“ ist also nicht das Problem, sondern die Lösung
- Dies hat Konsequenzen für jegliche Kommunikation zum Thema Informationssicherheit, auch z.B. für Awareness

Das Meerhäschen

- Kontrolle wird über alles gestellt
- Hochnäsig schaut man mit Glas dazwischen auf alles herab
- Drang nach dem absoluten Durchblick
- Im sicheren Abstand agieren, ohne sich emotional zu beteiligen (Schmerzvermeidung: Digitales statt Analogem)
- Endloses Versteckspiel (Obergewalt bewahren)
- Zersplitterung des Durch-Blicks

Endlichkeit des Blicks

- „Das Ganze ist mehr als die Summe ...“
- Je mehr Regeln, desto mehr Widersprüche, desto (paradoxerweise) mehr Auslegungsspielraum
- Kontrolle schafft Klima des permanenten Argwohns und Unterlaufen der Kontrolle (s.a. s.g. „Bilanzieren“ in Krisenzeiten der Finanzbranche)
- Pfählung kann Gegenmacht nicht Herr werden
- Stäete Verfeinern von Absicherung legt Entwicklung vollkommen still

Das Seelische ist und bleibt fehler- und lückenhaft

Gnade

- Durch Akt des Schenkens wird Berechnung und Verrechnen außer Kraft gesetzt
- Man muss den Worten trauen
- Selbst schlauer Fuchs braucht „Bedenkzeit“
- Schöpferisches Brachliegen eröffnet Raum für einen anderen Umgang mit der Wirklichkeit
- Aufschub und Kompromisse beleben die Starre
- Erst Umwege und ein unbedingtes Wollen führen aus der Isolation heraus

Meerhäuschen heute

- Vorratsdatenspeicherung + Anti-Terrorgesetze
- SWIFT + PAYD + RFID
- DB, Deutsche Telekom, Lidl & Co.
- Nacktscanner + Überwachungs-Kameras
- Blue-ray („Gnadenlos scharf“)
- Social Media („Zeigelust“ und „Tabu-Brüche“)
- etc.



z.B.
Wirkungs
analysen

CISO-Selbstbild

- »Aus der Abwehr in den Beichtstuhl« (2008)
- u.a. inkl. Analogien von CISO-Strategien in Märchen (»Froschkönig«) & Transformation in Typologie
 - »Zentrale Kontrollinstanz« (Fräulein Rottenmeier)
 - »Sicherheitsservice (Mutter Teresa)
 - »Stretworker« (Columbo)

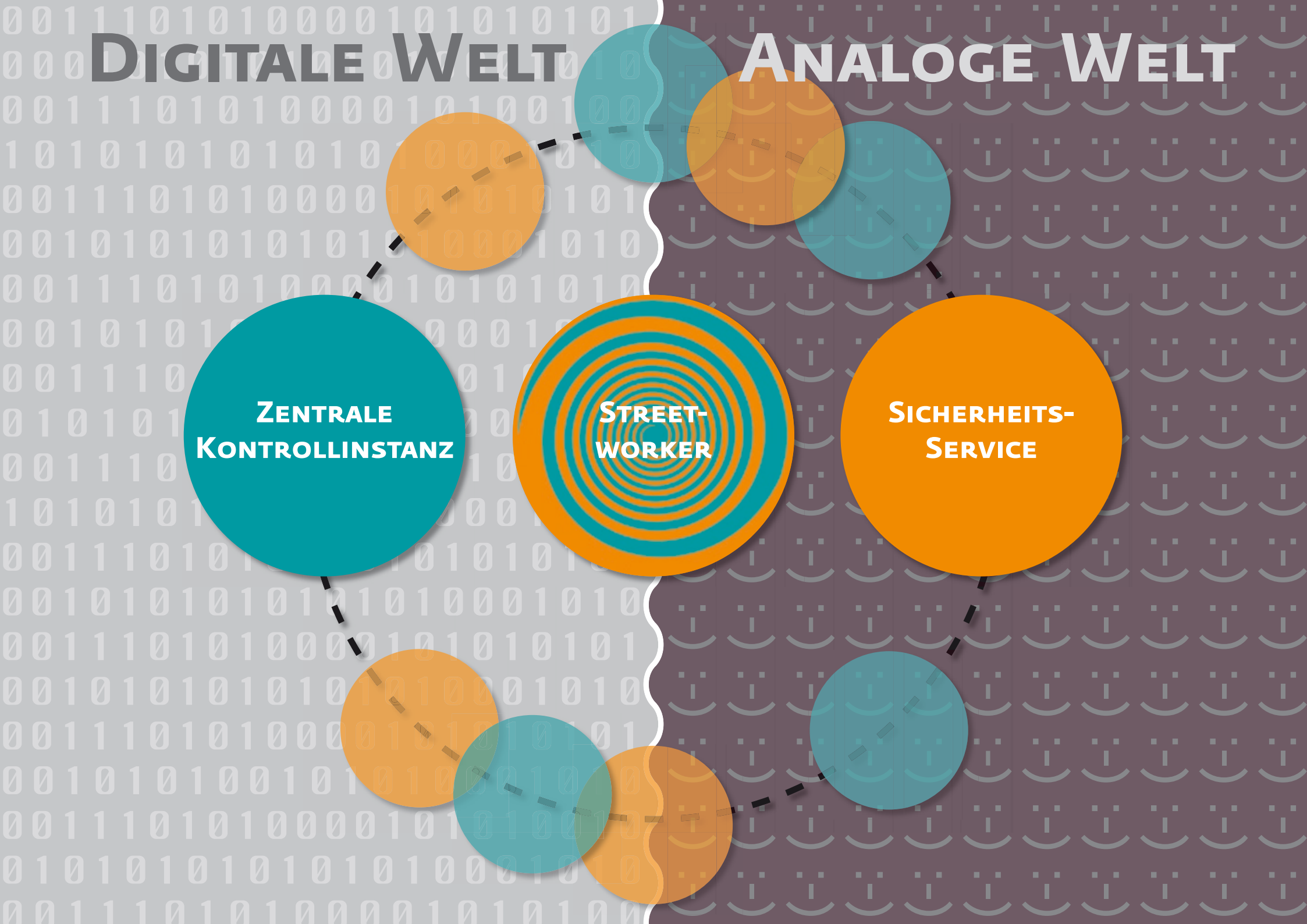
DIGITALE WELT

ANALOGUE WELT

**ZENTRALE
KONTROLLINSTANZ**

**STREET-
WORKER**

**SICHERHEITS-
SERVICE**





z.B.
Wirkungs
analysen

CISO-Fremdbild

- »Sicher – von oben. Qualitative Imageanalyse CISO & Co. – Security Manager und Informationssicherheit aus Sicht von Geschäftsführung, Management und Vorständen« (2009)



z.B.
Wirkungs
analysen

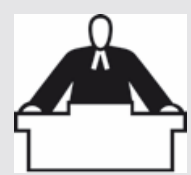
- Spaltung der Grundspannung von Stabilität und Innovation
- aufgrund Position andere Lösungsmöglichkeiten
- »Lex CEO« :Regelverstöße bei Entscheidern und Mitarbeitern unterschiedlich geahndet
- CISO und FK laufen Gefahr, sich zu ähnlich zu werden und sich in Machtkonflikten gegenseitig zu blockieren. (z.B. Delegation von ungeliebten Aufgaben & Vereinhaltung)

z.B.
Wirkungs
analysen

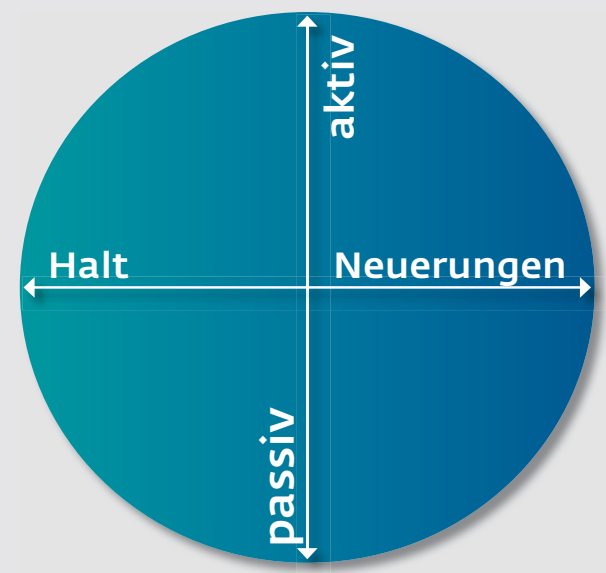
STREETWORKER



Selbstbewusster Vermittler



Streiter der Sicherheit



Kompetenter Sicherheits-Spezialist



ZENTRALE KONTROLLINSTANZ

Mahnender Kontrolleur



SICHERHEITSSERVICE



z.B.
Wirkungs
analysen

Interne Analysen

- Security-Maßnahmen sind davon geprägt, wie der einzelne Mitarbeiter das Unternehmen als Ganzes und seine Stellung innerhalb dieser Arbeitsfamilie erlebt, so dass jedes Unternehmen seine individuelle Sicherheitskultur produziert.
- Diese Sicherheitskultur ist untrennbar mit der jeweiligen Kultur eines Unternehmens verbunden
- Dies hat Konsequenzen für die Ausrichtung jeglicher Kommunikation, die Sicherheit zum Thema hat.



z.B.
Wirkungs
analysen

Interne Analysen

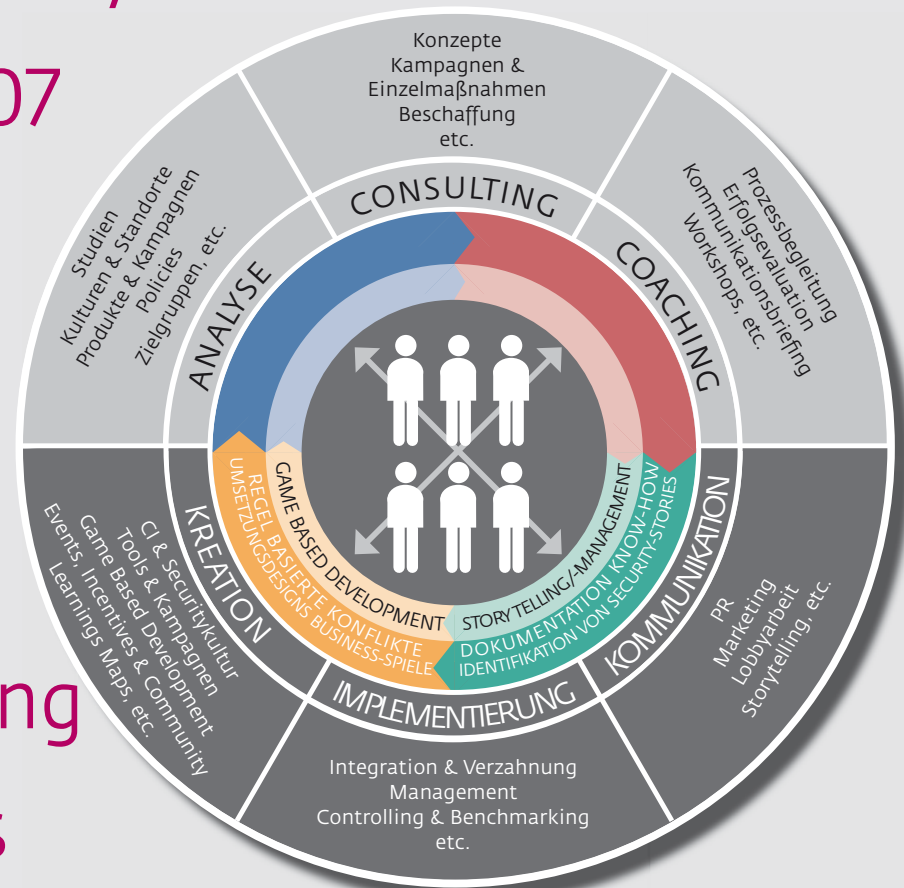
präsentieren Learnings über ...

- Sicherheitskultur
- Security-Painpoints
- bisherige Awareness-Maßnahmen
- Konzepte geplanter Maßnahmen
- Erfolge von Maßnahmen (qualitatives Benchmarking)

Tool »askit«

- z.B. »askit – awareness security kit«
- IT-Sicherheitspreis NRW 2007
- beschreibt Tools, Prozesse, Umsetzungsstrategien für
 - Sicherheitskultur-Analysen
 - Umsetzung in Kreation
 - Maßnahmen-Implementierung
 - Begleitung von Awareness

z.B. askit – awareness security kit



Tool »askit«

z.B. askit -
awareness
security kit

- »askitInterviews« (Wirkungsanalysen)
- »askitChange« (Benchmarking und qualitative Messung von Awareness-Entwicklungen)
- »askitMeta« (Security-Moderationstool für Workshops)
- »askitVision« (CISO-Coaching)
- »askitTouch« (Kommunikationsbriefing)
- »askitTalk« (Security-Blog zur qualitativen Online-Evaluation von Sicherheitskultur oder Awareness-Kampagnen)

»askit« »askitMeta«

z.B. Moderations-
karten

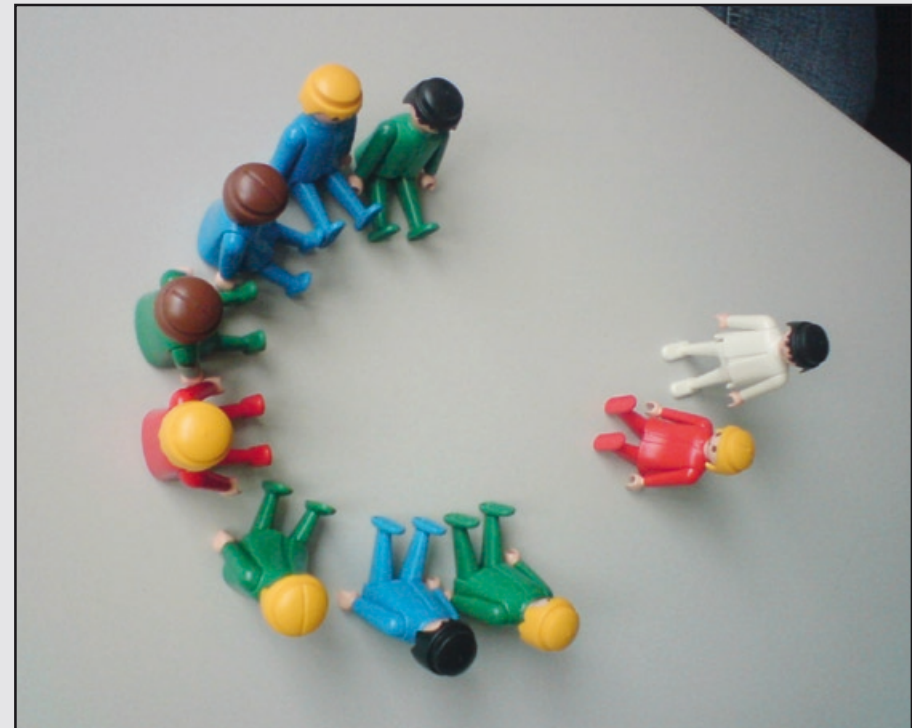
z.B. askit =
awareness
security kit



»askit« »askitMeta«

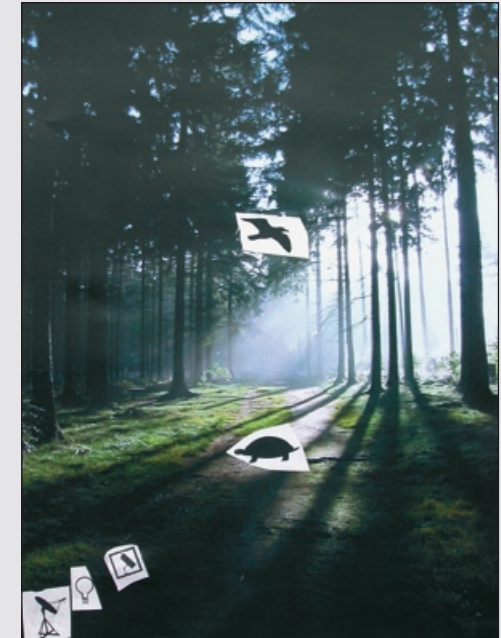
z.B. Aufstellungen Arbeitsumfeld

z.B. askit =
awareness
security kit



»askit« »askitMeta« z.B. Collagen von Arbeitsplätzen

z.B. askit =
awareness
security kit



z.B. Interventionen

- z.B. paradoxe Interventionen via „Passworthalter“ führen zur proaktiven Richtigstellung der Paradoxie durch die Mitarbeiter

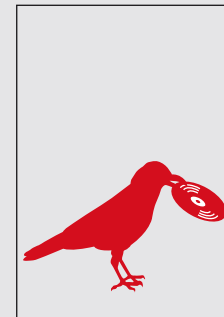


z.B. Storytelling

- z.B. Geschichten über Implementierung von Leitfiguren erzeugen Involvement (Beteiligt-Sein)



You make the difference – Information Security at



z.B. Game Based Development

- z.B. Lernspiele als Edutainment-Tool – auch als individuelles Planspiel zur Lösung regelbasierter Konflikte



Fazit

- Security, die »unsexy« ist, Security-Painpoints & -Krisen sind Teil von Kommunikationsstörungen und gesellschaftlicher Stillelegung (Abspaltung)
- Wissen um die Störungen unterstützt die Lösungen
- **Kontext:** Unternehmenskultur

Lösungen:

- Methodisches Vorgehen
- Unternehmen bzw. Mitarbeiter »auf die Couch«
- Entwicklungsangebote an Mitarbeiter

Fazit

Entwicklungsangebote = z.B. Security Awareness:

- Austausch fördern
- Betroffenheit erzeugen
- Konsequenzen demonstrieren

= **Marketing**: Zur Entwicklung gehört auch ein ausbalanciertes Security Awareness Marketing mit hohem Involvement!

Fazit

Awareness Marketing Next Generation wird erfolgreich durch ...

- Storytelling
(mit einer Balance aus Cover & Impact Story)
- kulturelle Valenz & Authentizität (Werte mitbewegen)
- = aktives Modellieren kulturellen Bedingungen, die möglichen »Entsicherungen« entgegen wirken

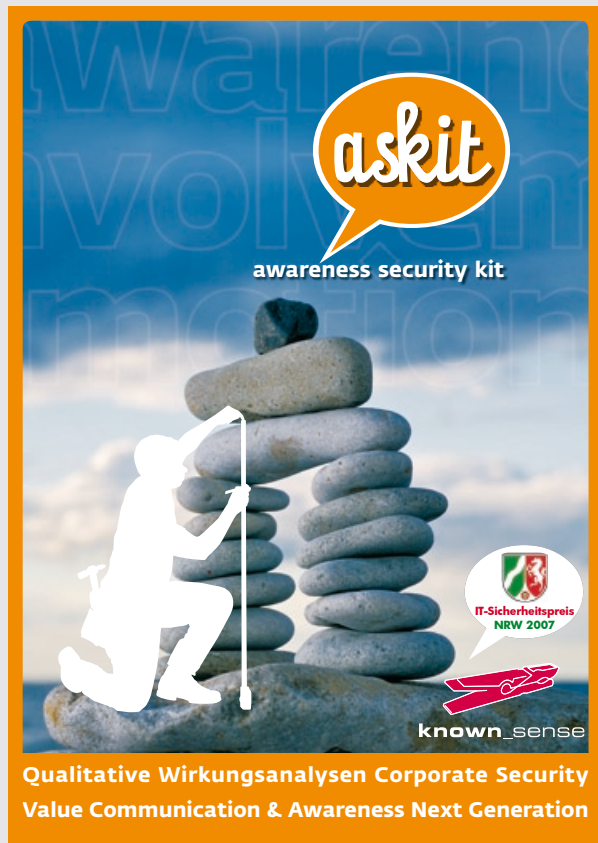
Fazit

- **Awareness Marketing** kann also dann erfolgreich sein ...
- wenn die Menschen die Awareness-Maßnahmen als komplette Geschichte erzählen können.
- wenn sie spüren, wofür die Awareness-Maßnahmen eintreten, welche Haltung sie verkörpern.
- wenn sie eine Konsistenz in Bezug auf die Werte ihres Unternehmens entdecken und die Werbung eingebettet ist in ein erlebbares Verhältnis von Unternehmens- und Sicherheitskultur, mithin weder die Menschen noch die Werte »verraten«, auf der sie aufbauen.

Sexy Security?

Touch them
if you can!

Sie wollen mehr wissen?



askit-Infofolder
(kostenfrei)



Buch »Security Awareness«
(Vieweg+Teubner, 49,90)

**Vielen Dank für Ihre
Aufmerksamkeit!**

pokoyski@known-sense.de

www.known-sense.de

www.known-sense.de/askit.pdf

www.aware-house.com