SECURITY AWARENESS @T-SYSTEMS.

Ivett Buzgó und Dr. Christoph Schog (Security Management T-Systems),
Dietmar Pokoyski (known_sense) – **Köln eco KG Sicherheit, 5. Juni 2013**

T · · Systems

ERLEBEN, WAS VERBINDET.

AWARENESS @TS: AUSGANGSLAGE.

Treiber von Security Awareness @T-Systems (1/2). Informationssicherheit & Compliance – unverzichtbar.

TS Int. Monitor 2010: Sonderauswertung ICT & Compliance

- ICT-Compliance spielt in den Unternehmen eine sehr große Rolle (72%).
- Tendenz in den nächsten Jahren weiter steigend (> 82%).
- 80% der Unternehmen nennen Probleme bei der Umsetzung von Compliance-Maßnahmen.
- Diese betreffen den gesamten Prozess (von mangelnder Akzeptanz durch Mitarbeiter bis hin zur Evaluierung des Erfolgs).

Detecon: Anforderungen TS-Kunden an Sicherheit & Datenschutz (2011)

- Kundenanforderungsmatrix benennt als Fokusthemen u. a.
  - „Sicherheitsabteilung/Organisation“
  - „Ansprechpartner zum Thema Sicherheit”
  - „ Cybercrime-Prävention”
  - „Schulungsnachweise TSI Personal”
- **Diese 4 Themen adressieren unmittelbar oder implizit Security Awareness**

Ohne strategische Awareness ist Security Management 2013 nicht mehr darstellbar.

AWARENESS @TS: AUSGANGSLAGE.

Treiber von Security Awareness @T-Systems (2/2). Global Accounts verlangen Awareness-Nachweis.

T-Systems Geschäfts-modell	Spezielle Anforderungen im Hinblick auf Standards und Policies.	▪ T-Systems ist die einzige vollumfänglich zertifizierte Business Unit im Konzern.
Dachzertifikat ISO 27001	Führende Standard für Informationssicherheit: Fortführung Zertifikat → weltweit konsistente Regelwerk erforderlich.	▪ Abweichungen führen zur Annullierung des Dachzertifikats und zum Verlust aller Zertifikate unter dem Dachzertifikat.
Mission Critical	FC (2008) →bei fehlender Zertifizierung 2010 ein Umsatzrisiko von € 3,3 Mrd. und Profitrisiko von € 547 Mio. (bis zu 50% Verluste bei Neukunden)	▪ Zertifizierung ist Voraussetzung für ein nachhaltiges Neukundengeschäft. ▪ Vor allem Kunden fordern zunehmend den Nachweis von Zertifizierungen (z. B. ISO 27001).
Sicherheits-strategie	Sicherheit→integraler Bestandteil sämtlicher Prozesse, d.h. FüKr und MA sind sich ihrer Verantwortung für Sicherheit bewusst.	▪ Erfolgsfaktoren, um unsere und die Kunden-Ressourcen wirksam zu schützen: ▪ nachgewiesene Sicherheitskompetenz ▪ positives Sicherheitsimage
Sicherheits-faktor Mensch	Neben der technischen und prozessualen Sicherheit ist das Sicherheitsbewusstsein der T-Systems Mitarbeiter von hoher Wichtigkeit.	▪ Global Accounts verlangen auch den Nachweis regelmäßig durchgeführter Security Awareness Maßnahmen.

AWARENESS @TS: AUSGANGSLAGE.

Sensibilisierungs-Historie seit 2005 (1/2)
Maßnahmen für mehr als 40 Tsd. MA in 60 Ländern.

Mission Security

- **2005** Start der Kampagne „Mission Security" auf Basis der Leitfigur James Bit
- Mit der Kampagne Start einer jährlichen Wirksamkeits-Messung (Online Awareness Umfrage) durch das Steinbeis Institut
- **2007** Zweiter Platz Sicherheitspreis Baden-Württemberg für „Mission Security"

my Security & Privacy Box

- **2009** Launch der „mySecurity & Privacy Box" für mehr als 5.000 Führungskräfte @TS
- Hierfür Kooperation sämtlicher Sicherheitsbereiche von T-Systems und der Group
- **2010** Übernahme des Tools durch die Group und Rollout in zahlr. weiteren Sprachen

Mission Security III

- **2012** Start des Maßnahmenpakets „Mission Security III", u. a. mit dem innovativen Awareness Circle Training SECURITY PARCOURS
- **2013** SECURITY PARCOURS u.a. in Deutschland Slowakei, Russland, Österreich, China, Malaysia, Singapur, Mexiko, Brasilien, USA
- **2014** geplant: Mitarbeiter-Video-Wettbewerb „Security in Motion – dein Clip zur Box"

Security Awareness @T-Systems: seit 2005 methodisch, strategisch und fortlaufend – aber auch nachweisbar!

AWARENESS @TS: AUSGANGSLAGE.

Sensibilisierungs-Historie seit 2005 (2/2)
Bsp. Moderationstool „mySecurity & Privacy Box“.

Grundlage der Regelvermittlung bei T-Systems

- **72 eCards** (in 13 Sprachen) zu wichtigen Sicherheits- und Datenschutz-Themen
- **Moderationsunterstützung** für Führungskräfte in Team-Settings
- **Regeln und Tipps:** „vorne“
- **Vertiefende Moderationsinhalte:** „hinten“, d.h Wissensfragen und weitere (für eine intensive Auseinandersetzung mit dem Thema)
- **Big picture:** Vergleiche, Metaphern sowie Verweisungen stellen Querverbindungen zwischen Sicherheit und Alltag her
- **Intuitive Struktur und hoher Funktionsumfang:** 6 anlassbasierte Hauptklassen, Stich- und Schlagwort-Index, zahlreiche Links
- **FAQ** mit Wissensfragen bzw. Fragen zum Handling und zur Moderation zur Begleitung

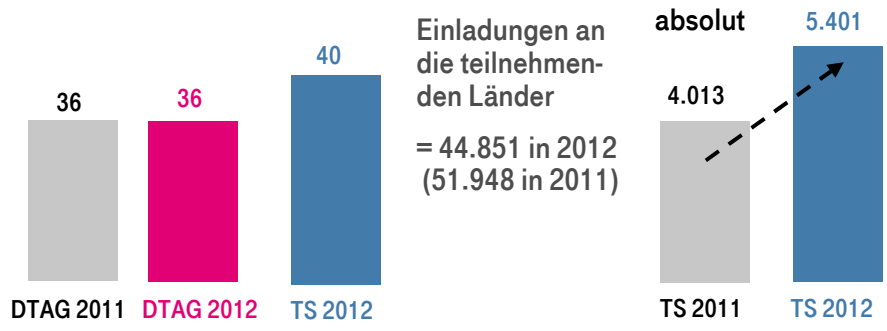
EXKURS: INTERNATIONALE ONLINE AWARENESS UMFRAGE.

AWARENESS-EVALUATION VIA GROUP.

AWARENESS @TS.

Internationale Online Awareness Umfrage (1/3). Seit 2005 jährliche Evaluation eines unabhängigen Instituts.

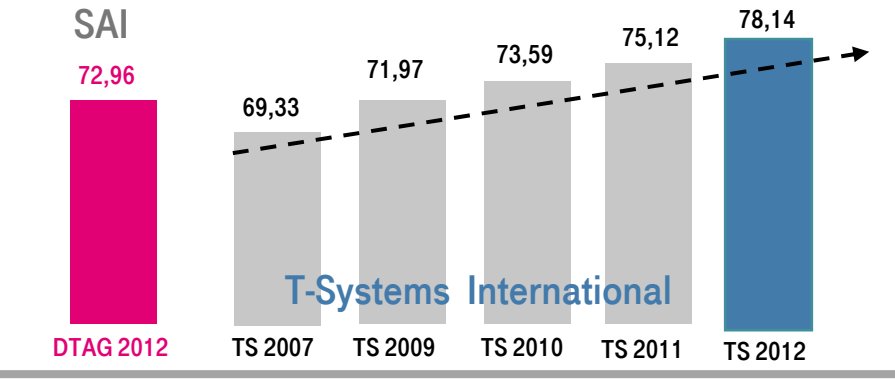
Response Rate: Hohe Antwortbereitschaft



Bei TS höher als in der Group

- Die Antwortbereitschaft bei T-Systems ist mit 40% im Vergleich zur Deutschen Telekom (36%) deutlich höher.
- Absolut hat sich die Bereitschaft zur Teilnahme 2012 mit 5.401 Mitarbeitern gegenüber 2011 mit 4.013 Mitarbeitern um 33% gesteigert.

Security Awareness Index (S.A.I.): Deutliche Steigerung



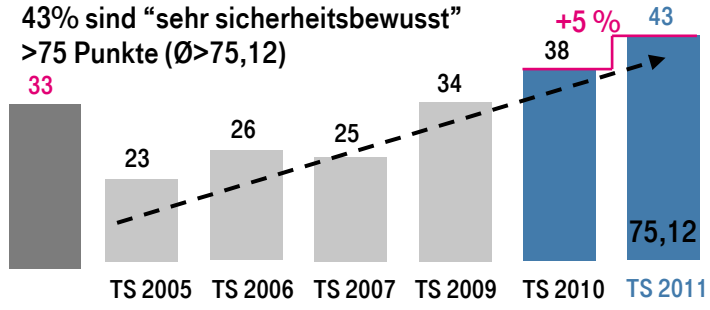
SAI bei TS höher als bei der Group

- T-Systems-Mitarbeiter erzielten 2012 78,14 % im Security Awareness Index (S.A.I.) eine Steigerung von mehr als 3 Punkten gegenüber 2011 (75,12 %).
- Seit 2007 ist bei T-Systems ein stetiger Aufwärtstrend (um mehr als 9 Punkte) zu verzeichnen.
- Wert liegt deutlich über DTAG-Niveau.

AWARENESS @TS.

Internationale Online Awareness Umfrage (2/3). Das Level der sehr Sicherheitsbewussten steigt.

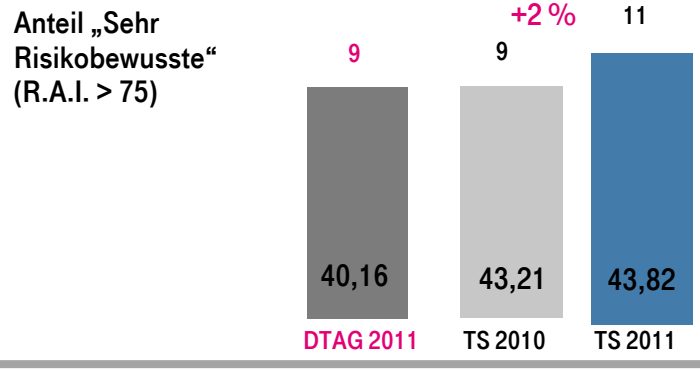
Level Security Awareness: Mehr Sicherheitsbewusste



Sicherheitsbewusste ansteigend

- Der Anteil der “sehr sicherheitsbewussten” Mitarbeiter (S.A.I. > 75): konnte seit 2007 ebenfalls kontinuierlich gesteigert werden.
- Hier liegt T-Systems deutlich vor der DTAG und gehört mit 43% (2011, +5% gegenüber 2010) zur Spitze.

R.A.I: Hohes Risikobewusstsein



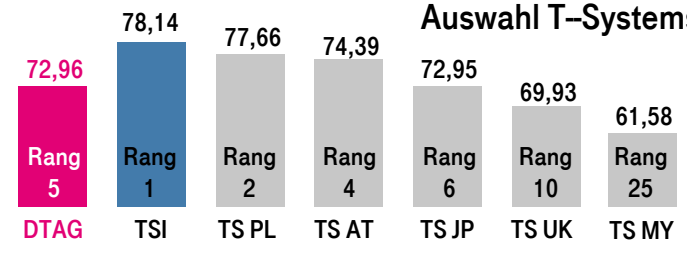
Anteil der Risikobewussten steigt

- Bei T-Systems Int. ist der Anteil der “Sehr Risikobewussten” im Vergleich zur Group überdurchschnittlich hoch.
- Die T-Systems-Mitarbeiter erreichen im Durchschnitt 43,82 von 100 möglichen Punkten auf der Risiko Awareness Skala. 11% erreichen mehr als 75 Punkte.
- Im Vergleich zur Vorjahresmessung ist der Anteil der „sehr risikobewussten“ Mitarbeiter 2% höher.

AWARENESS @TS.

Internationale Online Awareness Umfrage (3/3).
TS Int. ist sehr gut aufgestellt – Bedarf besteht in den LBUs.

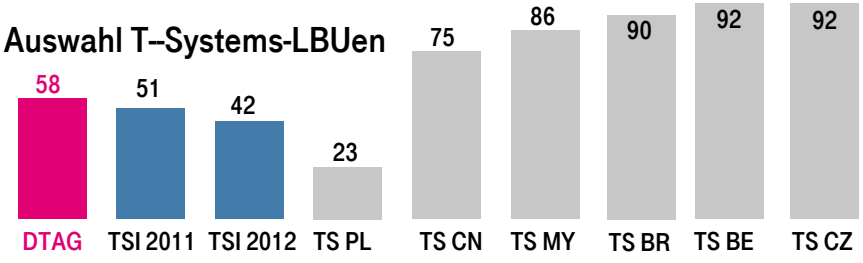
S.A.I.: TS International im Vergleich zu den LBUs



LBUs schlechter als die Group

- Außer TS Polen und Österreich schneiden die LBUs schlechter ab als der Durchschnitt der Group.
- Am schlechtesten schneidet TS Malaysia auf Rang 25 ab.

Risikopotenzial 2011-2012: Group und TS Int. im Vergleich



Risikopotenzial vor allem in LBUs

- Das Risikopotenzial zeigt den Anteil der MA an, die mit vertraulichen Daten umgehen.
- Bei TS Int. ist d. Risikopotenz. unterdurchschnittlich hoch (niedriger als bei d. Group)
- Hohes Risikopotenzial (>75) besteht u.a. in China, Malaysia, Brasilien, Tschechien
- Aufgrund der Korrelationen zu SAI-Werten ergibt sich Handlungsbedarf i. d. Ländern.

Der T-Systems Security Awareness-Fokus liegt 2013 bei den internationalen Standorten und auf dem erprobten Format SECURITY PARCOURS.

VON MISSION SECURITY ZUM SECURITY PARCOURS.

T-SYSTEMS SECURITY AWARENESS TOOLSET 2013.

AWARENESS @TS: METHODEN-ENTWICKLUNG.

Von Mission Security zum SECURITY PARCOURS. Awareness 3.0 – prozesshaft und involvierend.

Wissen – Oldschool (Awareness 1.0)

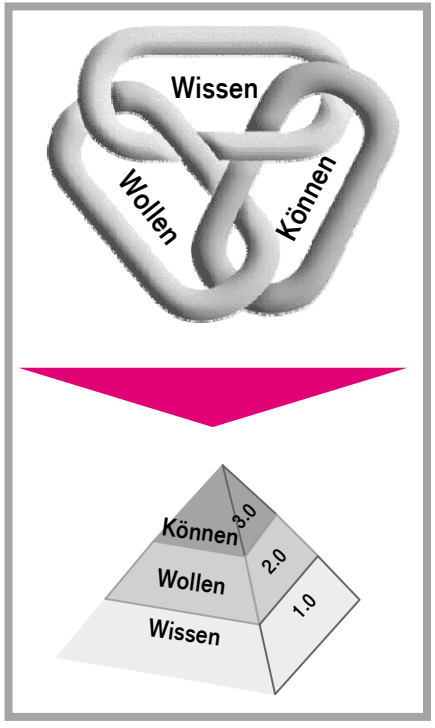
- Klassische Lerntheorie - Security Manager als Lehrer und Erzieher
- Wie: Konzentration auf Content-getriebenes Know-how, rein kognitive Wissensvermittlung
- Wodurch: Trainings, WBTs Intranet, Präsentationen (PowerPTs)

Wollen – Next Generation (Awareness 2.0)

- Marketing-basiert – Figur des James Bit als „Security-Partner“
- Wie: Klassische Promotion, Storytelling, emotional-motivierend
- Wodurch: Videos, Posters, Displays, Intranet, WBTs, Giveaways, Quizzes, Events etc. (z.B. Kampagne „Mission Security”)

Können – Awareness 3.0 = Mission Security III

- Soziale Aspekte & Team-orientiert - Securitymanager = Streetworker
- **Wie:** Prozess-basiert, Diskussionen auf Augenhöhe, hohes Involvement, Enabling zur eigenverantwortlichen Umsetzung
- **Wodurch:** SEC. PARCOURS, Deep Dive Workshops, mySecurity & Privacy Box, „Security in Motion“ – ein Video-Team-Wettbewerb, Flurfunk (erweitert um beste Ideen aus Awareness 1.0 and 2.0)



Awareness 3.0 hält den Menschen im Fokus, denn manchmal ist es zugunsten des umfassenden Überblicks besser, nach 2 Schritten vor wieder 1 zurückzutreten.

AWARENESS @TS: SYNERGIEN.

Zwei Welten –ganzheitliche Awareness.

1+1=1: TS profitiert auch von den Maßnahmen der Group.

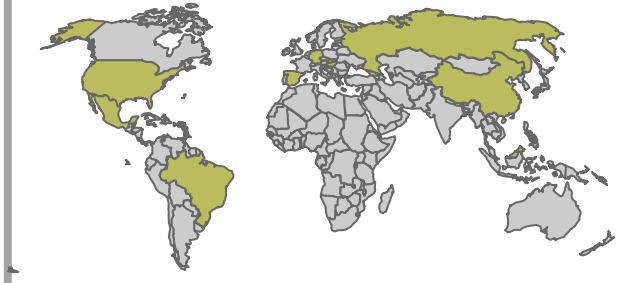
mySecurity Portal (inkl. mySecurity-Academy)

Deutsche Telekom AG/GBS

- Mehrsprachiges Kampagnenmaterial zu den Themen Zutrittsschutz, Social Engineering, Social Media u.v.m.
- Artikel, Videos, Audio-Podcasts, Selbsttests, Quizze, Spiele, Wettbewerbe u.v.m.
- Verfügbarkeit des begehbaren Planspiels „Bluff & Hack" für SECURITY PARCOURS (s. n. Folie)

+

Mission Security III-Toolset



T-Systems/SecM – z. T. mit GBS-Support

- SECURITY PARCOURS
- Online Awareness Umfrage, u.a. mit S.A.I.
- mySecurity & Privacy Box & App
- Deep Dive (Workshops)
- Security Community Cup
- mySecurity-Academy mit div. WBTs
- Außerdem: Marketing-Tools (Poster, Videos u.a.)

Beide Sensibilisierungsansätze, das mySecurity-Konzept der Group Business Security (GBS) UND Maßnahmen von T-Systems, ergänzen sich synergetisch.

AWARENESS @TS: SYNERGIEN.

TS profitiert auch von den Maßnahmen der Group. Bsp.: Bluff & HACK – das Social Engineering Game.

Bluff & Hack – das Game

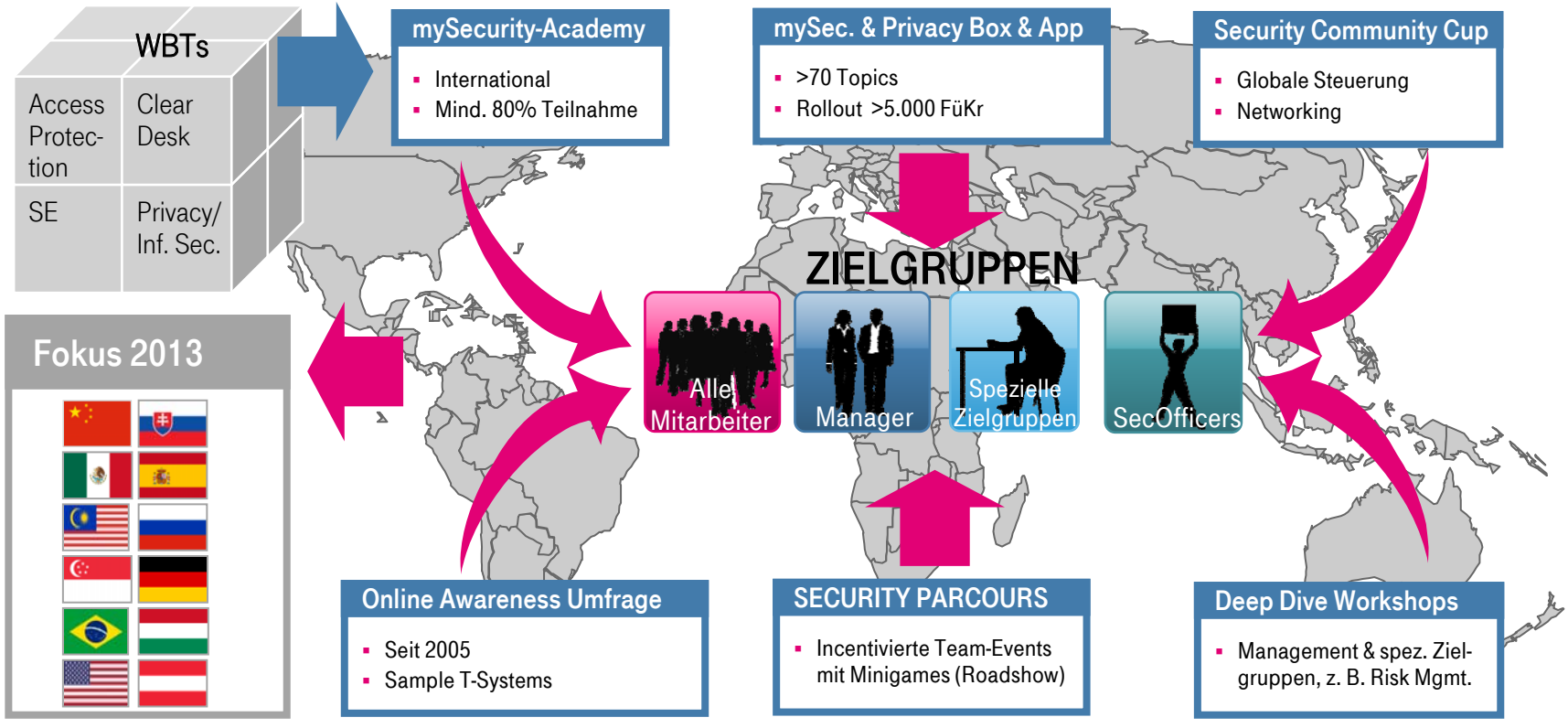
- Plan und Edutainmentspiel zu den Themenfeldern „Betrug und WiKri“
- Aus der von GBS/SAW der Deutschen Telekom produzierten Social-Engineering.-Kampagne „Moment mal.“ (2012).
- **Planspiel:** große Teppichversion (ca. 25 qm) für 3-5 Teams á 3-5 Mitspieler – zwingend moderiert
- **Edutainmentspiel:** große Teppichversion, Brettspiel oder downloadbare Schnittbogenversion (PDF) für 3-6 Einzelspieler.

Der SECURITY PARCOURS nutzt das ca. 20-50min. „Bluff & Hack“ als Add-on, bestritten von den Teamkapitänen nach Durchlaufen der Stationen.

SECURITY PARCOURS: AWARENESS@TS: TOOLSET.

Passende Kanäle für alle Themen/Zielgruppen.

Mission Security III-Toolset im Überblick.



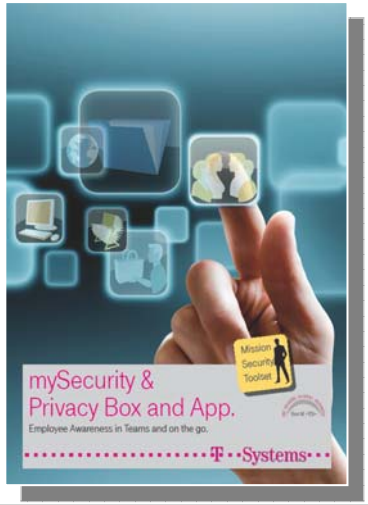
AWARENESS @TS: TOOLSET (2/2).

Promotiontools zur internen Vermarktung (Flyer).

Toolset-Flyer erklären FüKr u.a. Multiplikatoren (Awareness Ambassadeurs) die Details.

Deep Dive (Workshop)

mySecurity & Privacy Box bzw. App



mySecurity Toolset

SECURITY PARCOURS

Für jede BU/LBU zur richtigen Zeit das passende Werkzeug.

KERNMASSNAHME 2013.

DER SECURITY PARCOURS.

AWARENESS @TS.
SECURITY PARCOURS: Überblick (1/2).

Idee – Was ist der SECURITY PARCOURS?

- **Kontaktfördernd:** Involvierender Mix aus Lernen, Spiel und Story
- **Out of the box:** quadratisch – praktisch – gut!
- **Bewegung erzeugend**: je 4-10 Mitarbeiter- besuchen (synchron) 4-6 moderierte Security-Stationen
- **Spielerisch leicht:** Pro Station ein Miniplanspiel zum Regel-Einüben

Intention – Was steckt hinter dem SECURITY PARCOURS?

- **Clipformat:** Kurzer Aufwand (pro Kopf 45 - 75 Min)
- **Modular:** 7 Themen – 3 in Vorbereitung, jederzeit erweiterbar
- **Synchronizität:** sämtliche Stationen gleichzeitig verstärken die Lebendigkeit und stellen Bezüge her sowie die Visibility von Sicherheit

Benefits – Was bringt uns der SECURITY PARCOURS?

- **Lebendigkeit erweckt bzw. verstärkt positives** Security-Image
- **Teamformat** adressiert den Gemeinschaftssinn und Verantwortung
- **„Franchise-Verfahren“:** zentral koordiniert, aber von jeder LBU eigenständig zu managen

SUMMARY – Stationslernen mit Routentechnik!

- **Vergleichbar mit anderen Parcours wie z. B. Golf, Messe^n, Schatzsuche, denn es ist einfacher, sich etwas zu merken, wenn die klassische Routentechnik für bessere Memorierbarkeit sorgt und Regeln gemeinschaftlich thematisiert werden.**

Zielgruppen

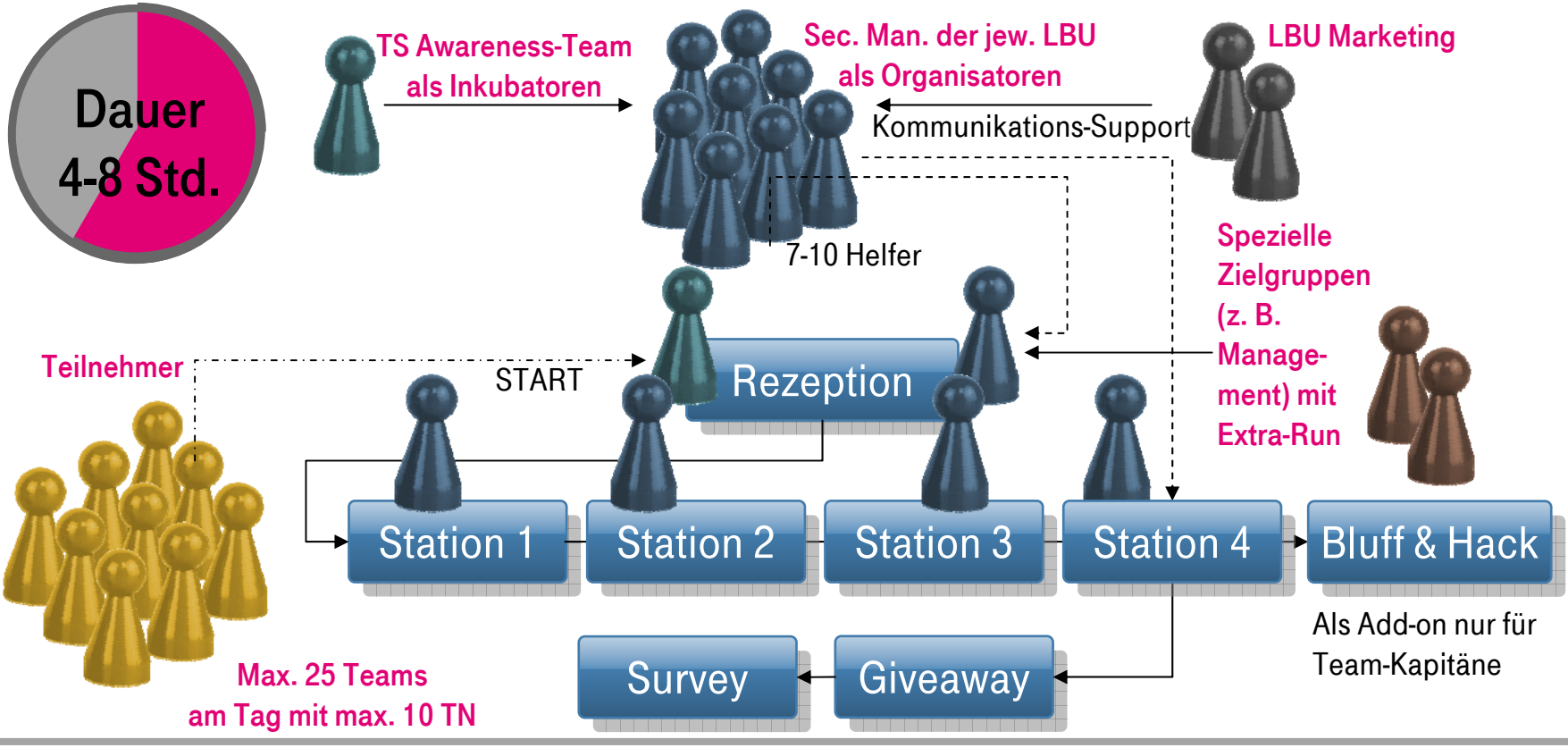
- Alle TS-Mitarb. (Awareness)
- Kunden (Best Practice)
- TS SecMan (Profilierung)
- max 250 Teilnehmer/Tag

Dauer

- Jedes Team 60-75 Min.
- Bei 5 Stationen und 5 Durchgängen/Tag 25 Gruppen mit je 10 MA = 250 TN

AWARENESS @TS.
SECURITY PARCOURS: Überblick (2/2).

Schematische Darstellungen von Aufgaben und Dramaturgie.



AWARENESS @TS.
SECURITY PARCOURS: Themen und Ablauf.

Verfügbare Stationen

- Informationssicherheit allgemein
- Social Engineering
- Social Media
- Clear Desk
- Klassifizierung
- Besucher & Ausweise
- Passwort Hacking
- ➔ **weitere in Vorbereitung**
- Sichere Server
- Security Incident Management
- Mobile Security

Jede Station (max. 15 Min) wird von einem Moderator im stets gleichem Ablauf moderiert.

4-7 Min.
ca. 35%.

Teil 1: Einführung, Regeln, Tipps & Tricks

- Begrüßung und Vorstellung
- Thema anhand der zugehörigen Themenkarten aus der mySecurity & Privacy Box (Vorderseite) erläutern
- D.h. die 3-5 wichtigsten Regeln erklären oder abfragen und persönliche Bezüge integrieren
- Moderationsfragen einstreuen

5-8 Min
(Spiel netto
2-5 Min.).
ca.. 45%

Teil 2: Durchführung Planspiel/Minigame

- Spiel erklären inkl. Zeitkontingent bzw. max. Punktzahl
- Spiel starten, Hilfestellung erteilen und Zeit überwachen
- Punkte auszählen und eintragen
- Ggf. mögliche Grauzonen besprechen (z. B. Doppel-Lösungen)

2-4 Min.
ca. 20%.

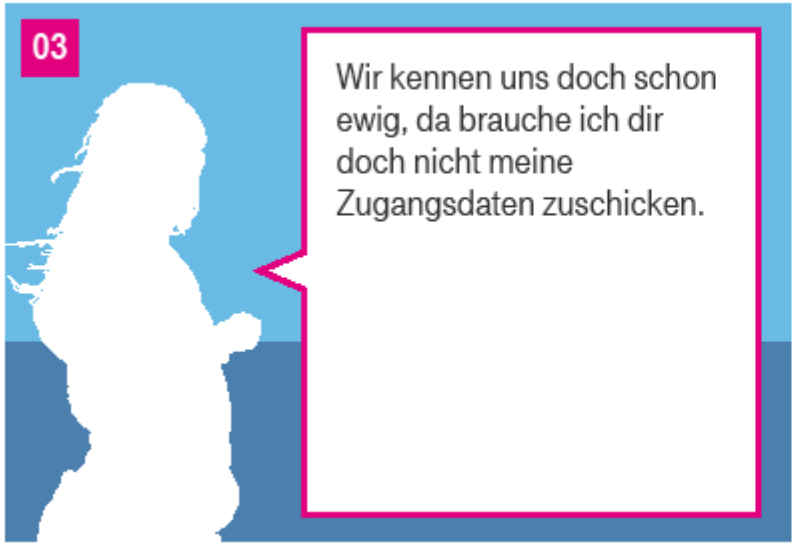
Teil 3: Debriefing bzw. Fragen und Verabschiedung

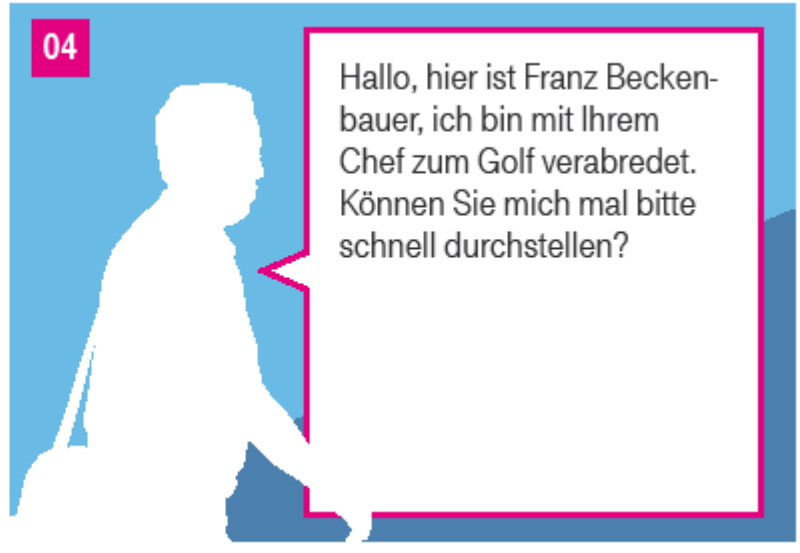
- Ergebnis des Minigame zum Anlass nehmen, Aktionen zu besprechen bzw. diskutierte Aspekte zu vertiefen
- Unsicherheiten ausräumen und auf weitere Hilfsmittel hinweisen (Links, Hotlines, Ansprechpartner, Maßnahmen, etc.)

AWARENESS @TS.

SECURITY PARCOURS: Moderationshilfen. Beispiel Station „Social Engineering“.

Zwei Beispielkarten aus dem Minigame.





AWARENESS @TS.

SECURITY PARCOURS: Anforderungen. Schlüsselfaktoren der Event-Kommunikation.

Schlüsselfaktoren	Dos	Don' ts
Moderatoren 	▪ Kommunikativ und auf Augenhöhe zu den Teilnehmern ▪ Authentisch und (selbst)reflektierend ▪ Spielerisch und involvierend ▪ Fachlich ausreichend, d.h. gegenüber den TN Sicherheit vermittelnd	▪ Fehlender Bezug zur Sicherheit allgemein bzw. zum moderierten Thema ▪ Ablesen bzw. am Konzept klebend und wenig authentisch
Minigames 	▪ Max. 5 Minuten ▪ Simpel, selbsterklärend, d.h. i.d.R. Mix aus bekannten Public Domain Regeln ▪ Interkulturell diversifizierbar und mobil ▪ Trigger für Diskussionen	▪ Zu komplex ▪ Digital bzw. wenig sinnlich oder haptisch ▪ desavouierend ▪ Nicht bewertbar im Rahmen der Incentivierung ▪ Zu voluminös (in Bezug auf Transport)
Location 	▪ Visibility on Location durch Positionierung im Eingangsbereich sichern ▪ Sichtbarkeit von Sicherheit auch jenseits der Stände (Promomaterial: Poster, Aufsteller etc.) ▪ Dadurch En-passant-Awareness auch bei den Nicht-Teilnehmern	▪ Zu klein >100 qm ▪ Zu groß (Einheit Gesamtbild geht verloren) ▪ Zu isoliert (keine Sichtbarkeit) ▪ Zu laut (Konzentration nicht möglich)

AWARENESS @TS.

SECURITY PARCOURS: Organisation. Aufgaben, Pflichten, Support.

TS Security Awareness Team

- Zentrale Weiterentwicklung des Formats als Mantelkonzept
- Zentrale Entwicklung von Themenständen und kompatiblen Minigames sowie passender Materialien
- Inkubation in Form der Sicherung von Verfügbarkeit sämtlicher Konzepte und Materialien sowie Steuerung der Voarb-Kommunikation (Telcos ab 6 Wochen vor Event)
- Beratung, Briefing (idR 1 Tag vor dem Event), Supervision und Dokumentation vor Ort
- Aufbereitung der Dokumentationen und Kommunikation nach Innen wie Außen

Organisatoren in den LBUs

- Konfektionierung von Themen bzw. Ständen auf Basis lokaler Incidents bzw. Notwendigkeiten
- Bei Premiere in der jew. LBU-Sprache Übersetzung der Moderationskonzepte, Minigames u.a. Materialien (Poster, Aufsteller, Promotionmedien)
- Interkulturelle Anpassung sämtlicher Inhalte
- Forderung Support durch Management und Marketing
- Akquise von Moderatoren/Helfern
- Bereitstellung von Security-Giveaways und Incentives
- Event-Promotion bzw. Teilnehmer Akquise
- Einladung von Kunden und ggf. Medien
- Betreuung des TS Security Awareness Teams vor Ort
- Durchführung Survey und Kommunikation nach Event

Grundlage ist eine Art „Franchisevereinbarung“ , d.h. die LBUs verpflichten sich, den SP innerhalb eines definierten Zeitraums eigenverantwortlich an diesem/weiteren Standorten in ihrem Land zu organisieren.

AWARENESS @TS.
SECURITY PARCOURS: Figuren-Familie.

TS International.: James Bit

- Ein virtueller TS-Mitarbeiter als Leitfigur der Kampagne „Mission Security“ mit eigenem XING-Profil zur Nutzung im Rahmen der Station „Password Hacking“

TS Hungary: Anna Naiv

- Eine neue TS-Mitarbeiterin, die in Bezug auf Informationssicherheit noch ahnungslos, aber hoch motiviert ist, mit eigenem Facebook-Profil.

TS Iberia: Carlos Noble

- Facebook-Profil von Carlos Noble, der Leitfigur des SECURITY PARCOURS in Barcelona

TS Russia: M. Rasteryasha

- Masha Rasteryasha - quasi der DAU bzw. die Anna Naiv Russlands

Es steht jeder LBU frei, eine eigene Story mithilfe einer kulturell passenden Leitfigur zu kreieren. Die so sukzessiv entstehende TS-Security-Familie soll zu einem späteren Zeitpunkt im Rahmen einer noch zu erstellenden „Vereinigungs“-Animation genutzt werden.

AWARENESS @TS.
SECURITY PARCOURS: Giveaways & Incentives.

Giveaways mit Security-Bezug und Incentives für die Mitglieder des Winner-Teams steigern Wohlgefühl beim Event und seine Memorierbarkeit.

AWARENESS @TS.

SECURITY PARCOURS: Feedback der Teilnehmer.

- „Eine sehr gute Idee, Athmosphäre und Spiele waren toll."
- „Nach dem Event habe ich mein Passwort sofort in ein sicheres geändert."
- „... Aufgaben unter ‚Zeitdruck' durchzuführen hat dazu beigetragen, dass wir Teilnehmer diese sehr konzentriert bewältigt haben. Dies simuliert die Stress-Situation im ‚Ernstfall'."
- „...eine absolut gelungene Veranstaltung, die mehr Teilnehmer verdiente. Die Teilnahme müsste eigentlich vom Management als ‚produktive Arbeitszeit' anerkannt werden!"
- „Gute Idee! Die Themen wurden persönlich und im Dialog vermittelt, es gab etwas zum Anfassen und bleibt deshalb besonders hängen."
- „Sehr gut gemacht, abwechslungsreich und hat mehr gebracht als ‚Powerpoint Schlachten'."

AWARENESS @TS.
SECURITY PARCOURS: live

Dokumentationen (in Auswahl)

Parcours on the road

- **2011/2012** Budapest, Debrecen, Košice, Barcelona, München
- **2013** bisher St. Petersburg, Woronesch, Wuhan, Peking, Leinfelden, Košice, Köln
- **25.6.** TS Mexico (Puebla)
- **15.-17.7.** TS Malaysia (Cyberjaya) und TS Singapur)
- **Aug.** TS NA (Scottsdale)
- **10.9.** TS Austria (Wien)
- **17.9.** Europäisches Planspielforum (Köln, koelnmesse, public)
- **8.-10.10.** TS Brasilien
- **30.10.** TS SI (Darmstadt)

AWARENESS @TS.
SECURITY PARCOURS: Fazit.

Chancen

- **Geringe Entwicklungs- und Materialkosten** in Relation zu z. B. aufwändigen Medien-Produktionen oder teuren WBT-Lizenzen
- **Hohe Memorierbarkeit** bei den TN durch Nutzung der klassischen Routen-Methode und positiv assoziierter Gemeinschaftserlebnisse
- **Hohes Involvement** der TN durch Erzeugung von Spannung und Teambuilding-Qualitäten
- **Große Aufmerksamkeit** bei allen Zielgruppen – auch beim Management - aufgrund der belegbaren Nachhaltigkeit des Stationen-lernens und der Einzigartigkeit des Formats
- **Dialog:** Verbesserter Austausch int. Sec. Man.
- **„Franchise-Qualitäten“:** selbständige Durch-führung durch die LBUs nach „Erst-Inkubation“

Risiken

- **Reichweite** geringer als bei „Stellvertreter-Medien“ wie Portalen, AV-Medien, Print u. a., d.h. verhältnismäßig hoher Ersaufwand bei Inkubation (Reisekosten in Abhängigkeit von Entfernung bzw. hoher personeller Einsatz)
- **Teilnahme-Quote** stets abhängig vom Multiplikations-Effekt, die der jew. Veranstalter erzeugt (erzwungene Teilnahme vs. erfolgreiche Akquise durch ggf. eine aufmerksamkeitsstarke Promotion)

Security Parcours – das passendes Werkzeug für nachhaltige Sensibilsierung und den vielstimmig geforderten Awareness-Nachweis sowie ein innovatives Format, das nach Innen wie nach Außen für eine hohe Aufmerksamkeit sorgt.

AWARENESS @TS.
Noch Fragen?

Dr. Christoph Schog
International Security, Security Awareness
T-Systems International GmbH

Tel. +49 2408 9569 680
E-Mail: christoph.schog@t-systems.com

Ivett Buzgó
Security Management
T-Systems International GmbH

Tel. + 36 1381 8750
E-Mail: ivett.buzgo@t-systems.com

Dietmar Pokoyski
Geschäftsführer known_sense
Externe Awareness-Beratung & Kreation

Tel. +49 2203 183 1618
E-Mail: pokoyski@known-sense.de

VIELEN DANK!

T · · Systems

ERLEBEN, WAS VERBINDET.