Security Awareness in der betrieblichen Praxis

take aware, Essen 28.04.2022

HECOM
Security Awareness Consulting

HINTERGRUND

Ziele und Umsetzung

Ziele: Wie wird Security Awareness geplant und umgesetzt?

- was waren die kritischen Erfolgsfaktoren?
- welche Erfahrungen wurden dabei gesammelt?

Umsetzung:

- 2009 & 2011
- 2015 in Zusammenarbeit mit dem BSI

Teilnehmende Organisationen und Befragte

Teilnehmende Organisationen

- Teilnehmer: 17 Organisation
- Branchen: divers
- Größe der Organisationen: >5000 MA
- Ansässig in D/A/CH

Befragte

- Tätig als Sicherheitsverantwortliche (8) oder Awareness Spezialisten (4)
- Eigene Rolle im Awareness-Vorhaben: Projektleitung (9 von 21 Antworten)

ERGEBNISSE

Anlass, Initiierung und Verantwortung für das Vorhaben

Was hat Sie zur Umsetzung Ihres Awareness-Vorhabens veranlasst?

- Präventivmaßnahme (16) vs. aktueller Sicherheitsvorfall (1)

Wer (welche Organisationseinheit) hat das Awareness-Vorhaben veranlasst[1]?

- IT-/Informations -/Unternehmenssicherheit:12
- Unternehmensleitung: 8
- Risk Management: 2
- IT-/Informations -/Unternehmenssicherheit und Unternehmensleitung: 5x
- Unternehmensleitung und IT-Betrieb: 1

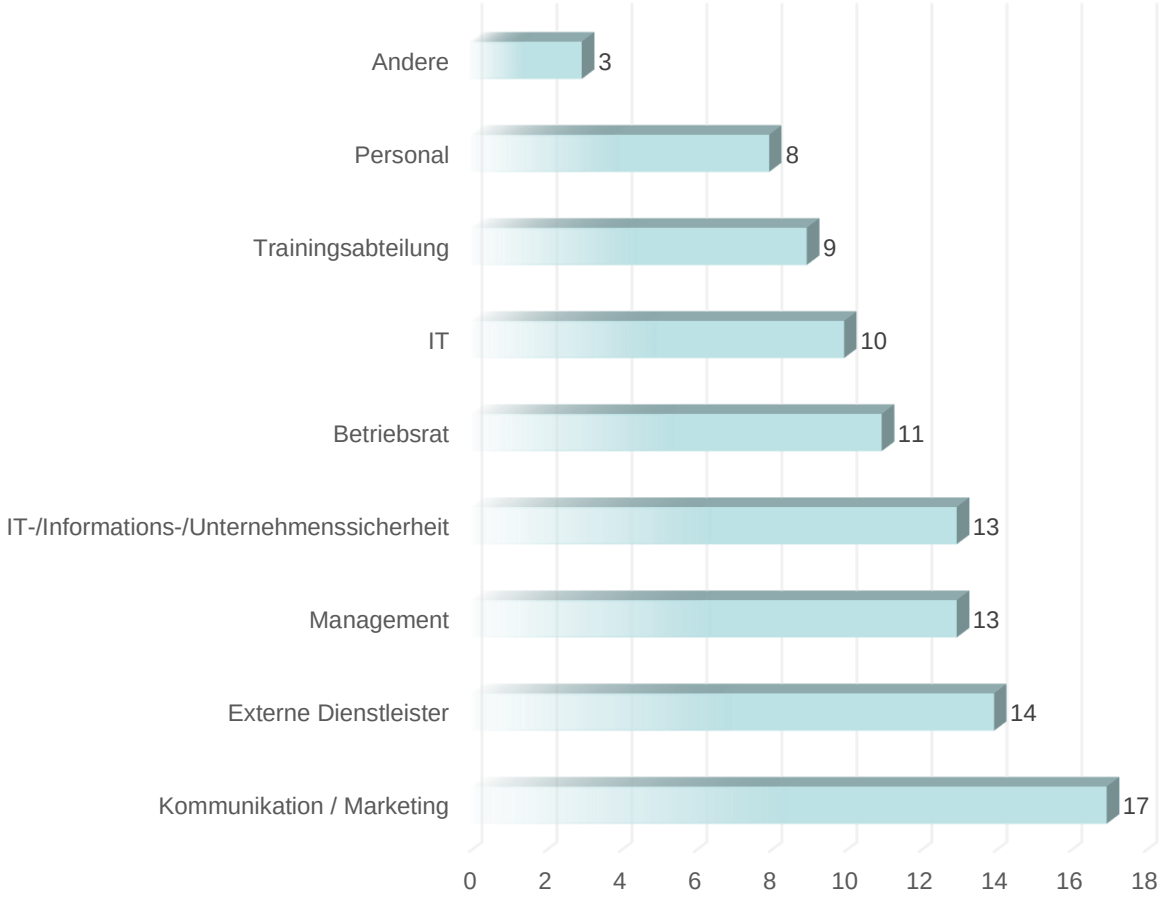
Welche Organisationseinheit war für die Umsetzung verantwortlich[2]?

- IT-/Informations -/Unternehmenssicherheit: 14

[1] Anzahl Antworten: 25

[2] Anzahl Antworten: 19

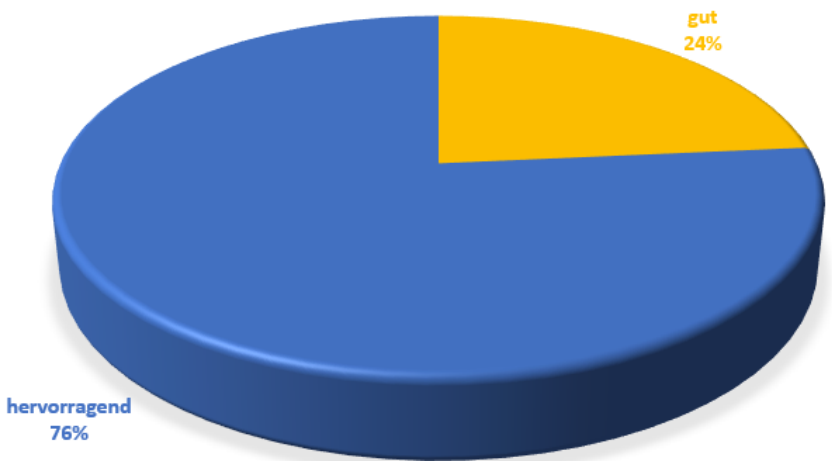
Welche Abteilungen und Partner wurden einbezogen?



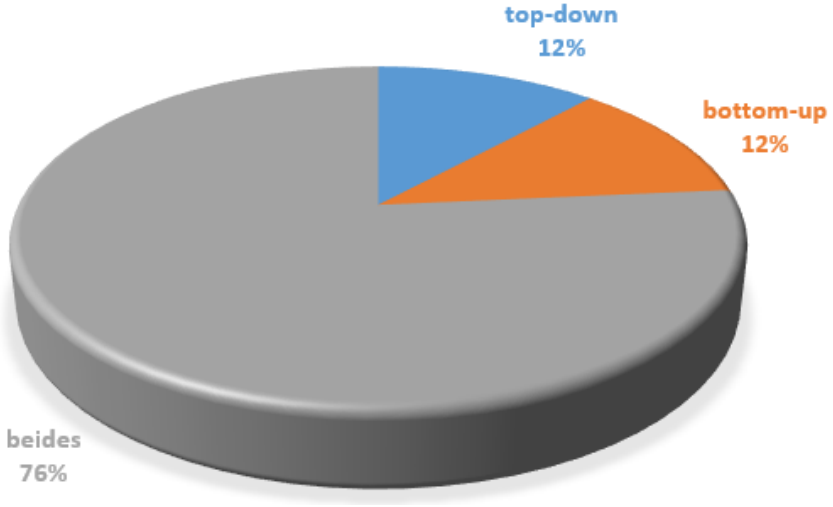
Anzahl der Nennungen: 98

Managementunterstützung und Umsetzung

Wie beurteilen Sie die Unterstützung durch das Management[1]?



Wie haben Sie Ihr Awareness-Vorhaben umgesetzt?



Durchschnitt aller Antworten: 1,76

[1] fünfstufige Skala von unzureichend (-2) bis hervorragend (+2)

Unternehmenskulturelle Besonderheiten

Welche unternehmenskulturellen Besonderheiten wurden in Ihr Awareness-Vorhaben einbezogen?

- bei überwiegender Mehrheit (14/17) **nicht** einbezogen

- Anpassung des Programms an (generelle) kulturelle Unterschiede:
  - Übersetzung in andere Sprachen (5)
  - Gestalterische Anpassung an die Belange anderer Kulturen (1)

- wenn Unternehmenskultur berücksichtigt:
  - Bewusstes Hinwegwegsetzen via „freche / lockere Sprache“ (2)
  - Bezugnahme zu „Weiterbildung & ständiges Lernen“ (1)

Herausforderungen

Benennen Sie die größten Herausforderungen im Verlauf Ihres Vorhabens

- Sehr vielfältige Antworten

- Mehrfachnennungen:
  - Corona
  - Das Thema Information Security bislang unbekannt im Unternehmen
  - Umsetzung in einer Vielzahl von Ländern
  - Genereller „information overload“ bei den Mitarbeitern
  - Erreichbarkeit der Mitarbeiter in der Produktion (mit digitalen Medien)
  - Knappe Ressourcen / Budget

Eingesetzte Medien: E-Medien und Print-Medien

E-Medien[1]	
Intranet	29%
E-Mail	21%
Blogs	17%
Andere	17%
Newsletter	16%

Print-Medien[2]	
Poster	26%
Broschüren	19%
Handzettel / fact sheets	17%
Präsentationen	17%
Mitarbeiterzeitschriften	11%
Andere	9%

[1] Anzahl Antworten: 58

[2] Anzahl Antworten: 53

Eingesetzte Medien: Lernen und sonstige Medien

Lernen[1]	
Workshops / lunch & learn	35%
Reines cbt/wbt	27%
Blended learning	19%
Klassisches Präsenztraining	16%
Andere	3%

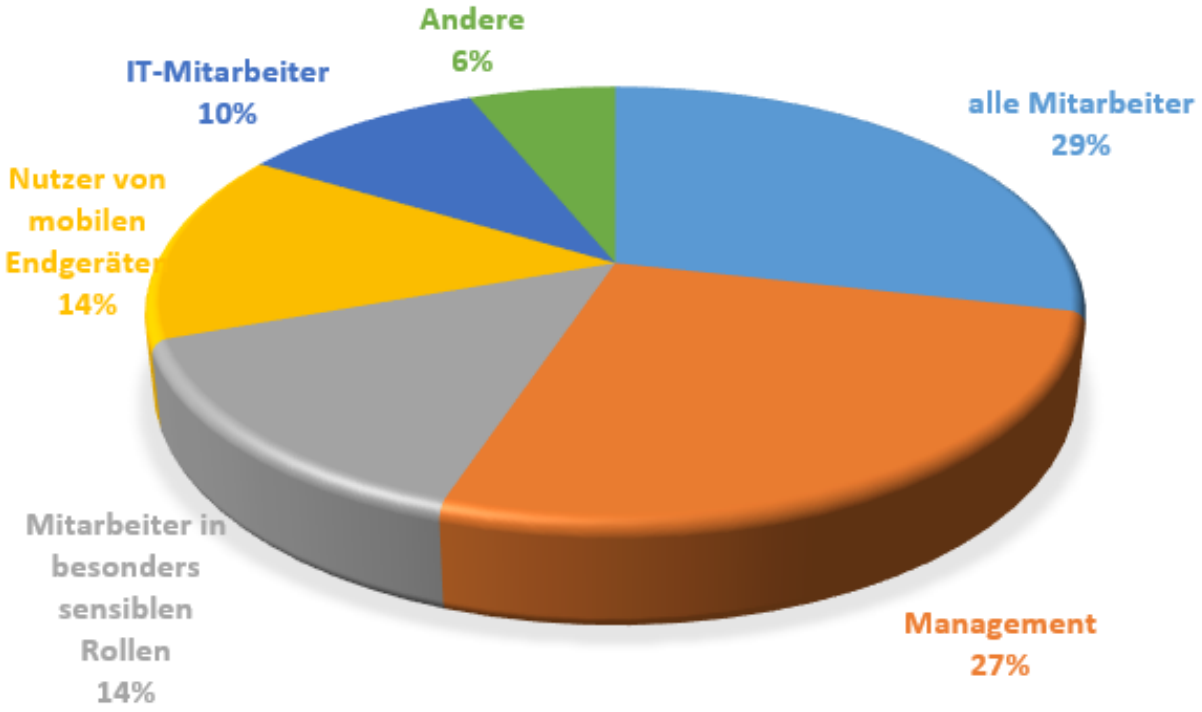
Sonstige Medien[2]	
Event (Roadshow, Messe, etc.)	22%
(Gewinn-)Spiele	18%
Filme/Videos	18%
Statement der GL	18%
Promotionmaterial	16%
Andere	6%

[1] Anzahl Antworten: 37

[2] Anzahl Antworten: 67

Adressierte Zielgruppen

Welche Zielgruppen waren Ihnen dabei besonders wichtig?



[1] Anzahl Antworten: 49

Ziele

Welche Ziele sollten mit Ihrem Awareness-Vorhaben erreicht werden?

„Verstehen, was InfoSec bedeutet & warum es wichtig ist“

„Bedrohungen adressieren & Risiko reduzieren“

„Bewusstsein schärfen/steigern“

„Positive Wahrnehmung & Akzeptanz schaffen“

„Zum Handeln motivieren“

Erfolgsmessung

Wie haben Sie den Erfolg Ihres Awareness-Vorhabens gemessen?

Rückmeldungen/ persönliches Feedback der Mitarbeiter

Auswertung von simulierten Phishingkampagnen

Teilnahmequoten an Websessions, e-learnings, kampagnenrelevanten Veranstaltungen/Aktionen

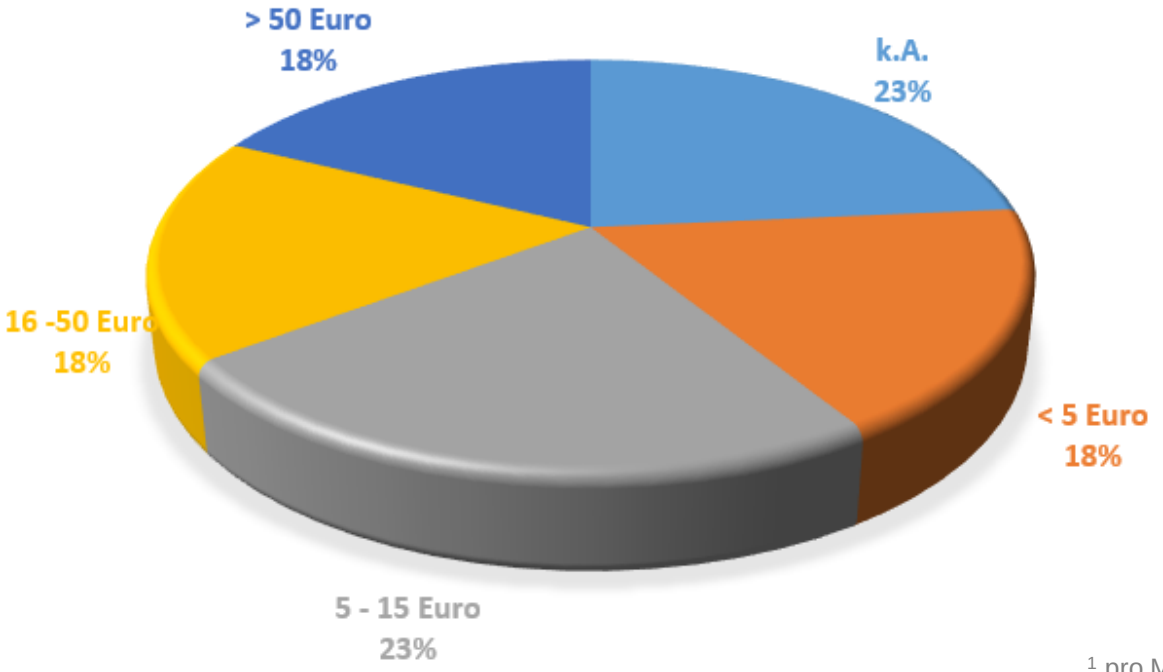
Anzahl gemeldeter (sicherheitsrelevanter) Tickets

→ **Ganz unterschiedlich - ohne klare „Favoriten“**

Kosten

Wie hoch beziffern Sie die Kosten Ihres Vorhabens (ohne Ausfallzeiten)?

- Kosten pro Mitarbeiter variieren zw. 0,3 und 100 €, Ø 29 €[1], Median 16 €



[1] pro Mitarbeiter

Ausblick

Mit welchen Aktivitäten wird ihr Awareness-Vorhaben zukünftig weiter geführt?

- Sehr divers, leichter Schwerpunkt im Bereich Phishing
- Fast alle Teilnehmer setzen auf Kontinutität

Quelle: www.pixelio.de

Erfolgsfaktoren

Benennen Sie die **fünf** wichtigsten Erfolgsfaktoren für Security Awareness

- Ganz unterschiedliche Erfolgsfaktoren genannt.

  - Top 3: kontinuierliche Kommunikation bzw. Awareness Maßnahmen (10%)
    Zielgruppenspezifische Ansprache (7%)
    Unterstützung durch das Management (6%)

[1] Anzahl Antworten: 82

Vielen Dank für Ihre Aufmerksamkeit

Michael Helisch

HECOM Security Awareness Consulting

Rheingoldstraße 12, D-85579 Neubiberg
+49 (0)172 272 4 272
helisch@hecom-consulting.de
www.hecom-consulting.de