



marim consult
business consultancy for professionals



Angebot einer IT Sicherheit Awareness Kampagne

im Rahmen einer ISO 27000 Zertifizierung

Nieder-Olm, August 2018



ANGEBOT

Strukturierte und
individuelle
Sensibilisierung
der Mitarbeiter
für IT Security
und Datenschutz

- Zielsetzung
- Nutzen
- Umfang Beratung
- FIREWALL Awareness Spieleset
- Preise
- Lieferungen und Leistungen
- Kontakt



ZIELSETZUNG

Zertifizierung einer unternehmensweiten Sensibilisierung aller Mitarbeiter nach **ISO 27001 A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung** als Teil eines ISMS

- Das ISMS wird die verschiedenen Teilaspekte der **Informationssicherheit** – im speziellen die Vertraulichkeit, Integrität, Informationsverfügbarkeit – **gewährleisten und aufrechterhalten**
- Das ISMS wird einem externen **Audit** bezogen auf die zu erfüllenden Anforderungen
- Das ISMS wird von der **Owner zuverlässig** durchgeführt
- Das ISMS wird **auf allen Personen** unterstützt
- Das ISMS wird durch eine abgestimmte **Awareness Kampagne** alle relevanten Teile einer Sensibilisierung des gesamten Personals sicherstellen (A.7 Personelle Sicherheit, ISO 27001, 27002)

Interesse?
Nehmen Sie Kontakt auf!
Info (@) marim.de

ZIELSETZUNG

Eine **Awareness Kampagne** als Teil der ISO 27000 Zertifizierung zeigt, dass Informationen zu den **kritischsten Werten** gehören und jeder Mitarbeiter für deren **effektiven Schutz** verantwortlich ist

- Die Awareness Kampagne liefert eine nachhaltige und messbare **Erhöhung des Bewusstseins** für IT- Sicherheitsrisiken und deren Konsequenzen
- Die Awareness Kampagne ermöglicht eine **frühzeitige Erkennung** und korrekte **Behandlung** von Sicherheitsvorfällen
- Die Awareness Kampagne sensibilisiert Mitarbeiter für das **Tagesgeschäft** und die **Informationssicherheit**
- Die Awareness Kampagne vermittelt das **Vorgehen zur Sensibilisierung aller Mitarbeiter** für Informationssicherheits-Risiken
- Die Awareness Kampagne **verbessert den Schutz** beim Umgang mit Informationen – beruflich wie privat

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

NUTZEN

Aufbau einer nachhaltigen IT-Sicherheits-sensibilisierung nach ISO 27002 7.2.2
Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit

- **Reduzierte Haftungsrisiken** im Bereich des Datenschutzes und der Informationssicherheit stärken das Kundenvertrauen
- Identifizierte **Risiken** werden **gezielt verringert**, gesteuert und abgesichert
- Ein Informations- und Transparenz als Sicherheitslage
- **Wettbewerbsvorteile** durch Entwicklungen u
- **Aktiver Schutz**
- Einbindung von
- **Breite und nachhaltige Sensibilisierung** der Mitarbeiter für IT-Sicherheit und Datenschutz
- **Einzigartiges Preis-Leistungsverhältnis** durch den breiten und nachhaltigen Wissensaufbau der Mitarbeiter

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

UMFANG BERATUNG

1. Aufnahme der **aktuellen Bedrohungslage** des Unternehmens verschiedener Abteilungen des Unternehmens

Cyber-Sicherheits-**Check der individuellen Bedrohungslage** (ohne Vor-Ort-Begehung) nach Standard des Bundesamtes für Sicherheit in der Informationstechnologie (**BSI**) und der Information Systems Audit and Control Association (**ISACA**)

- ...
- ...
- ...
- ...
- ...
- ...
- ...

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

UMFANG BERATUNG

2. Festlegen eines **Konfrontations-
trainings intern /
extern** (optional) als
Teil der Awareness
Kampagne auf Basis
der Erwartungen
und gesteckten Ziele

Kritische Assets der Informationen, IT-Systeme, Prozesse und Mitarbeiter festlegen, die vor Gefahren geschützt werden müssen:

Kundendaten, Einkaufskonditionen, Transaktionsdaten, Payment-Informationen, Mitarbeiter-/Gehaltsdaten, Strategische Dokumente, Gesellschafterbeschlüsse, Geschäftsverträge, etc.

Vorführung der **Anforderungen** an die IT-Sicherheit und Partner sowie externe Gefahren d

- ...
- ...
- ...
- ...
- ...

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

UMFANG BERATUNG

3. Schwerpunkte
**Sensibilisierung
definieren** -
Schäden für
entstehen durch die
Verletzung der
**Verfügbarkeit,
Integrität und
Vertraulichkeit**

Ausarbeitung des individuell auf das Unternehmen angepasste Awareness-Trainings für Multiplikatoren und Mitarbeiter für die Schutzziele. Basis bilden die **unternehmensindividuellen Angriffsvektoren** aus den Ergebnissen des Cyber-Sicherheits-Checks und des Konfrontationstrainings

- ...
- ...
 - ...
 - ...
 - ...
- ...
- ...

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

UMFANG BERATUNG

4. Sensibilisierung durch **nachhaltige Wissensvermittlung** für Multiplikatoren und Mitarbeiter durch gezielte und abgestimmte Schulungen

Schulungen werden auf Basis des Cyber-Sicherheits-Checks und des Konfrontationstrainings sowie der individuell abgeleiteten Schutzziele als **Frontal- und/oder Gruppenunterricht (Active-Learning-Methode)** durchgeführt

- ...
- ...
- ...
- ...
- ...
- ...
- ...

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

UMFANG BERATUNG

5. Der Wissensstand muss **regelmäßig überprüft und Schulungen angepasst** werden

Nachhaltige Erhöhung des Awareness-Erfolges und des Bewusstseins für IT- Sicherheitsrisiken und deren Konsequenzen basiert auf wiederkehrenden und anhaltenden Maßnahmen

- ...
- ...
- ...
- ...
- ...
- ...
- ...

Interesse?

Nehmen Sie Kontakt auf!

Info (@) marim.de

FIREWALL AWARENESS SPIELESET

- Schwerpunkte **nach Bedarf**
- Regelmäßige **Aktualisierung** und **Überprüfung**
- **Nachhaltiger** Wissensaufbau
- Hohe Aufmerksamkeit
- **Verständlicher** Wissenstransfer

**Angebot abhängig von
Stückzahl und Design**

- **Multiplikatoren-Spieleset für 4-8 Spieler**
Spielplan, Figuren und Würfel in stabiler Spielebox

- **Basiskartensatz mit 40 Karten:**

...IT-Grundsicherung:

- Zugang zum Computer sichern
- Software aktuell halten
- Antivirenprogramm
- Firewall-Software
- Datensicherung

...Passwortschutz:

- Ein Passwort pro Benutzerkonto
- Keine Multi-User-Passwörter
- Nutzerauthentifizierung
- Starke Passwörter

...und viele mehr

- **Multilingual** und Anpassung an Marketingmaßnahmen möglich
- **Individuelle Kartenerweiterungssätze**
auf Basis des Cyber-Sicherheits-Checks und des Konfrontationstrainings



KONTAKT



Markus J Neuhaus M.A.
EPM, GB, CSP
T: +49.6136.953954
M: +49.151.65128885
markus.neuhaus (a) marim.de



marim consult
business consultancy for professionals



DISCLAIMER / HAFTUNGSAUSSCHLUSS

Haftung für Inhalte

Die auf Seiten dargestellten Beiträge dienen nur der allgemeinen Information und nicht der Beratung in konkreten Fällen. Wir sind bemüht, für die Richtigkeit und Aktualität aller in der Präsentation enthaltenen Informationen und Daten zu sorgen. Für die Korrektheit, Vollständigkeit, Aktualität oder Qualität der bereitgestellten Informationen und Daten wird jedoch keine Gewähr übernommen.

Die Haftung für den Inhalt der abrufbaren Informationen (Haftung für Links) wird ausgeschlossen, soweit es sich nicht um vorsätzliche oder grob fahrlässige Falschinformation handelt. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Haftung für Links

Wir sind für den Inhalt von Webseiten, die über einen Hyperlink erreicht werden, nicht verantwortlich. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich. Wir machen uns die Inhalte dieser Internetseiten ausdrücklich nicht zu eigen und können deshalb für die inhaltliche Korrektheit, Vollständigkeit und Verfügbarkeit keine Gewähr leisten. Wir haben bei der erstmaligen Verknüpfung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Wir sind aber nicht dazu verpflichtet, die Inhalte, auf die wir unserem Angebot verweisen, ständig auf Veränderungen zu überprüfen, die eine Verantwortlichkeit neu begründen könnten. Erst wenn wir feststellen oder von anderen darauf hingewiesen werden, dass ein konkretes Angebot, zu dem wir einen Link bereitgestellt haben, eine zivil- oder strafrechtliche Verantwortlichkeit auslöst, werden wir den Verweis auf dieses Angebot aufheben, soweit uns dies technisch möglich und zumutbar ist.

Urheberrecht

Die auf diesen Seiten erstellten Logos, Inhalte und Werke unterliegen dem deutschen Urheberrecht. Sämtliche Beiträge Dritter sind als solche gekennzeichnet. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Kopien von diesen Seiten sind nur für den privaten Bereich gestattet, nicht jedoch für kommerzielle Zwecke.