Bundesministerium
des Innern

SICHER GEWINNT
BAköV · BSI
SICHER GEWINNT

Sicher gewinnt!

Sensibilisierungsinitiative für Informationssicherheit in der Bundesverwaltung

Teil I - Der Sensibilisierungsleitfaden

BAköV

Sicher gewinnt!

Sensibilisierungsinitiative für Informationssicherheit
in der Bundesverwaltung

Teil I

Der Sensibilisierungsleitfaden

Bundesakademie für öffentliche Verwaltung
www.bakoev.de

Inhaltsverzeichnis

Vorwort

Der vorliegende Leitfaden soll IT-Sicherheitsbeauftragten bei der Konzeption einer Sensibilisierungsinitiative zur Informationssicherheit als praktische Arbeitshilfe dienen. Neben der gedruckten Ausgabe wird der Leitfaden auch unter www.bakoev.bund.de/sicher-gewinnt und auf der Lernplattform www.lernplattform-bakoev.bund.de online veröffentlicht.

Teil I liefert die theoretischen Grundlagen zum richtigen methodischen Vorgehen, während Teil II Der Werkzeugkasten geeignete Instrumente und Materialien zur praktischen Durchführung darstellt. Die Ergebnisse der Kampagne werden als Teil III Die Initiative - Resümee und Ausblick vorgelegt.

In allen drei Teilen werden besonders nützliche Inhalte durch drei verschiedene Symbole hervorgehoben:

Das Icon »Information« (Symbol i) steht für wertvolle Hinweise zum Umgang mit dem Leitfaden und liefert weitere Quellen.

Das Icon »Tipp« (Symbol !) steht für Vorschläge zum praktischen Vorgehen.

Das Icon »Beispiel« (Symbol Glühbirne) steht für Beispiele zur Nutzung und Anwendung.

Wir wünschen Ihnen viel Spaß und Erfolg bei der Umsetzung der Initiative in Ihrem Haus.

Kontakt BAköV Lehrgruppe 5

1. Sensibilisierungsinitiativen für Informationssicherheit in der Bundesverwaltung

Die aktuellen Herausforderungen für die Informationssicherheit in der öffentlichen Verwaltungsind groß: Die Vernetzung von IT-Systemen, das steigende Datenvolumen sowie kriminelle Angriffe aus dem Internet stellen das Sicherheitsmanagement vor immer neue Aufgaben. Allein mit moderner Technik lässt sich Informations- und Datensicherheit in diesem Umfeld nicht realisieren. Eine aktive Mitarbeit aller Beschäftigten in den Behörden ist unverzichtbar. Umfragen haben in den vergangenen Jahren beispielhaft gezeigt, dass die größte Gefahr für die Sicherheit der Daten und Informationen vom Fehlverhalten der eigenen Belegschaft ausgeht. Informationssicherheit kann demnach nur erreicht werden, wenn alle beteiligten Personen Teil des Sicherheitsprozesses sind und das auch dauerhaft bleiben. Voraussetzung ist natürlich ein entsprechendes Bewusstsein der Nutzerinnen und Nutzer in den Behörden für das Thema Informationssicherheit — auf allen Ebenen. IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung können dieses Ziel mit der Durchführung von Sensibilisierungsinitiativen erreichen. Dabei sollen über den Einsatz verschiedener motivierender und anleitender Maßnahmen die Beschäftigten dazu angeregt werden, sensibel und sicher mit den ihnen anvertrauten Daten sowie der vorhandenen Informationstechnik umzugehen. Außerdem sollen sie befähigt werden, Gefährdungen frühzeitig zu erkennen und an das IT-Sicherheitsteam weiterzugeben.

In der Reihe „Sicher gewinnt!“ werden für die Planung, Durchführung und Evaluation von Sensibilisierungsmaßnahmen Tipps und Empfehlungen gegeben.

Teil I Der Leitfaden
Teil II Der Werkzeugkasten
Teil III Die Initiative - Resümee und Ausblick

Die Reihe ist online in der jeweiligen aktuellen Version unter www.bakoev.bund.de/sicher-gewinnt.

1.1. Rahmenbedingungen für IT-Sicherheitsbeauftragte

Entsprechend der Ziele des »Nationalen Plans zum Schutz der Informationsinfrastrukturen« ist es im Umsetzungsplan für alle Behörden der Bundesverwaltung Pflicht, IT-Sicherheitsbeauftragte zu benennen. Die IT-Sicherheitsbeauftragten sind auf der Ebene der Behördenleitung angesiedelt und für den gesamten Sicherheitsprozess innerhalb der Behörde verantwortlich. Um die ausreichende Qualifikation der IT-Sicherheitsbeauftragten zu gewährleisten, haben die Bundesakademie für öffentliche Verwaltung (BAköV) und das

Bundesamt für Sicherheit in der Informationstechnik (BSI) den Fortbildungsgang »IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung« (mit Zertifikat) entwickelt. IT-Sicherheitsbeauftragte der unterschiedlichen Behörden werden alle fünf Jahre durch die Fortbildung zertifiziert und weiter qualifiziert.

Zusätzlich hat die BAköV die vorliegende Reihe „Sicher gewinnt!“ zur Durchführung von Sensibilisierungsinitiativen erstellt, um die IT-Sicherheitsbeauftragten und das Informationssicherheitsteam bei ihrer Arbeit praktisch zu unterstützen.

1. 2. Aufgaben von IT-Sicherheitsbeauftragten

Als IT-Sicherheitsbeauftragte sind Sie in Ihrer Behörde für die Erstellung eines Schulungs- und Sensibilisierungskonzeptes zum Thema Informationssicherheit verantwortlich. Dazu gehört auch die Planung, Koordination, Durchführung und Evaluation von Sensibilisierungskampagnen. Dabei ist die Integration der Belegschaft sowie die Berücksichtigung von deren individuellen Stärken und Schwächen im Umgang mit Informationstechnologie ein wesentlicher Faktor für Sie und Ihr Sicherheitsteam. Zentraler Bestandteil Ihrer Aufgabe ist deshalb die Kommunikation mit allen Beschäftigten.

Unterstützen Sie sie durch verlässliche Informationen und die Beantwortung von Fragen rund um das Thema Informationssicherheit. Berücksichtigen Sie in der Ansprache das Hintergrundwissen Ihres Gegenübers und scheuen Sie sich im Zweifelsfall nicht, auch einfache Abläufe wiederholt zu erklären. Je intensiver Sie auf die individuelle Situation der einzelnen Personen eingehen, desto größer wird auch das Vertrauen der Belegschaft in Sie als IT-Sicherheitsbeauftragte/r sein. Das gewonnene Vertrauen wird Ihnen nützen, wenn Sie die Beschäftigten im Rahmen einer Kampagne für das Thema Informationssicherheit sensibilisieren und zur aktiven Mitarbeit motivieren wollen.

Weitere ausführliche Informationen zur Planung und Durchführung von Schulungen zur Informationssicherheit bieten Ihnen die IT-Grundschutzkataloge M 3.5 und M 3.45 des BSI (www.bsi.de).

Ebenfalls hilfreich ist der Leitfaden zur Security Awareness der European Network and Information Security Agency (ENISA) unter www.enisa.europa.eu. Dort finden Sie auch nützliche Checklisten, Fragebögen und Arbeitspläne.

2. Informationssicherheit als dynamischen Prozess in die Sicherheitskultur integrieren

Die Angriffstechniken auf die Informationssicherheit werden immer ausgefeilter und verändern laufend ihre Formen — man denke nur an Methoden wie Phishing oder Social Engineering. Deshalb muss sich auch der Sicherheitsprozess in Behörden dynamisch weiterentwickeln. Dazu gehören nicht nur die stetige Aktualisierung der technischen Sicherheitskomponenten, sondern auch die regelmäßige Information und die kontinuierliche Einbindung aller Beschäftigten.

Eine Herausforderung für IT-Sicherheitsbeauftragte ist es deshalb, einen fortlaufenden Fluss von Sensibilisierungsmaßnahmen zu entwickeln und umzusetzen, die das Thema Informationssicherheit dauerhaft als Teil der Organisations- und Sicherheitskultur etablieren. Immer dann, wenn eine Maßnahme abgeschlossen ist, muss eine neue Aktion das Thema wieder aufgreifen und in das Bewusstsein der Beschäftigten zurückholen.

Auf die Weise stellen Sie sicher, dass Informationssicherheit innerhalb der Organisation als Thema »lebendig« bleibt und eine positive und nachhaltige Auseinandersetzung der Belegschaft mit dem Thema erreicht werden kann.

3. Phasen der Sensibilisierungsinitiave

Um ein strukturiertes Vorgehen bei der Umsetzung einer Sensibilisierungsinitiative zu erreichen, sollten Sie und Ihr Sicherheitsteam die Umsetzung der Sensibilisierungsinitiative in aufeinander folgende Phasen gliedern. Ihre Verfahrensweise orientiert sich dann am etablierten Vorgehen im Projektmanagement und ist besonders zielführend.

1. Phase: Bedarfsermittlung

Am Anfang Ihres Konzepts steht die Analyse der Ausgangssituation. Hier bestimmen Sie, welche spezifischen Problemstellungen sich hinsichtlich der Informationssicherheit in Ihrer Behörde ergeben und welche Ressourcen Sie nutzen können oder zur Verfügung stehen.
Weitere Informationen liefert Kapitel 3.1.

2. Phase: Vorbereitung

Im Rahmen der Vorbereitung legen Sie die konkreten Ziele Ihrer Sensibilisierungsinitiative fest und definieren messbare Zielvorgaben. Eine wichtige Rolle spielt die von der Struktur Ihrer Behörde abhängige Identifizierung der richtigen Zielgruppen und die Einbindung der Behördenleitung, der Beauftragten für Datenschutz und Geheimschutz, Korruption, Gleichstellung und der Personalvertretungen.
Weitere Informationen liefert Kapitel 3.2.

3. Phase: Maßnahmenauswahl

Für die Durchführung einer Sensibilisierungsinitiative stehen Ihnen unterschiedliche Instrumente und Maßnahmen zur Verfügung.

Entsprechend Ihrer Bedarfsermittlung, der identifizierten Dialoggruppen und der zur Verfügung stehenden Ressourcen wählen Sie in dieser Phase die geeigneten Aktionen aus. *Entsprechende Informationen liefert Kapitel 3.3.*

Bei der Maßnahmenauswahl empfiehlt es sich, auf Teil II Der Werkzeugkasten zurückzugreifen.

4. Phase: Durchführung

Sie setzen die ausgewählten Maßnahmen nach Ihrem Projektplan in Ihrer Behörde um. *Weitere Informationen liefern die Kapitel 3.4. und 3.5.*

5. Phase: Evaluation

Mit Fragebögen, Gesprächen und Checklisten können Sie den Erfolg Ihrer Arbeit messen und eine laufende Feinjustierung Ihrer Arbeit vornehmen. *Weitere Information liefert Kapitel 3.6.*

Dieses in Phasen gegliederte Vorgehen und der gezielte Einsatz der Materialien haben den Vorteil, dass Sie Ihr Konzept stark bedarfsorientiert anpassen und maßgeschneiderte Lösungsansätze verfolgen können.

Zusätzlich helfen Ihnen die „Sicher gewinnt!-Moderationskarten“ bei der Vorbereitung und Planung von Sensibilisierungsmaßnahmen in Ihrer Behörde (siehe Teil II Der Werkzeugkasten).

3.1. Bedarfsermittlung (Phase I)

Bevor Sie mit der konkreten Planung beginnen, müssen Sie sich einen Überblick über die spezifische Ausgangssituation Ihrer Behörde im Hinblick auf die Informationssicherheit verschaffen. Gliedern Sie diese erste Bestandsaufnahme in drei Teile:

1) Situation der Informationssicherheit aus Sicht der Sicherheitsbeauftragten
2) Einstellung und Wissensstand der Beschäftigten, Organisations- und Beschäftigungsstruktur der Behörde
3) Verfügbare bzw. erforderliche personelle, technische und finanzielle Ressourcen

Beachten Sie bei allen drei Punkten immer die spezifischen Bedingungen in Ihrer Behörde. Dazu gehören bestehende Regeln, Verbote, Gebote, Richtlinien sowie technische und organisatorische Maßnahmen zur Informationssicherheit. Ziehen Sie außerdem Ihr Sicherheitskonzept und die Leitlinie zur Informationssicherheit heran.

1) Situation der Informationssicherheit aus Sicht der Sicherheitsbeauftragten

Der erste Schritt zur Umsetzung einer erfolgreichen Sensibilisierungsinitiative besteht darin, die grundsätzlich vorhandenen Problemfelder der Informationssicherheit in Ihrer Behörde zu definieren. Nehmen Sie sich dafür ausreichend Zeit, denn nur wenn Sie von Anfang an die wichtigen Erfordernisse der Sensibilisierung identifizieren, können Sie im weiteren Verlauf den Bedarf für individuelle Maßnahmen feststellen. In diesem Zusammenhang lohnt es sich auch, aktuelle Quellen über die Informationssicherheitslage (zum Beispiel (z.B.) Informationen des BSI) zu berücksichtigen. Beantworten Sie sich in Stichworten folgende Fragen:

- Was sind die größten Sicherheitsprobleme der Behörde für die Informationssicherheit?
- Gibt es für die Informationssicherheit besonders sensible Bereiche oder Abteilungen?
- Wo sind die sensiblen Informationen/Daten Ihrer Behörde?

- Welche Sicherheitsprobleme sind in jüngster Vergangenheit aufgetaucht?
- Verfügen die Beschäftigten der Fachabteilungen Ihrer Meinung nach über ausreichend Sachverstand im Umgang mit der Informationstechnik?
- Konnten die Ursachen für die Probleme auf Fehlverhalten von Beschäftigten zurückgeführt werden, wenn ja, auf welches?
- Gibt es bei den Beschäftigten Unterschiede in der Kompetenz beim Umgang mit Informationstechnik?
- Welches Fehlverhalten haben Sie bei den Beschäftigten am häufigsten wahrgenommen?

Teil II Der Werkzeugkasten bietet Ihnen zusätzlich eine Checkliste sowie einen Fragebogen zur Bedarfsermittlung an, mit denen Sie die Bestandsaufnahme in Bezug auf die Standardinhalte zur Informationssicherheit bei Bedarf weiter konkretisieren können.

Nun haben Sie die wichtigsten Themenfelder notiert und können diese entsprechend ihrer Priorität für die Informationssicherheit gewichten. Es ist im Anschluss sicherlich sinnvoll, zu bestimmten Punkten die Meinung anderer entsprechend qualifizierter Kollegen und Kolleginnen einzuholen, etwa von den Mitgliedern des Sicherheitsteams, den Beauftragten aus der Leitungsebene oder von den Personalvertretungen.

Nutzen Sie Ergebnisse der internen Hotline des Help Desk. Diese leistet den Beschäftigten bei Schwierigkeiten in Verbindung mit der Informationssicherheit am Telefon »Erste Hilfe«. Dort werden die jeweiligen Anfragen und der weitere Umgang mit der Problemstellung innerhalb der Behörde dokumentiert.

Anhand dieser zusätzlichen Informationen können Sie Ihre eigenen Einschätzungen überprüfen und ggf. um weitere wichtige Punkte ergänzen.

2) Einstellung und Wissensstand der Beschäftigten

Nachdem Sie die grundsätzlichen Problemfelder eingegrenzt haben, müssen Sie den konkreten Sensibilisierungsbedarf der Beschäftigten feststellen, um später die richtigen Maßnahmen einzuleiten. Machen Sie sich in diesem Zusammenhang klar, dass nicht jeder sicher und souverän mit Informationstechnik und Daten umgeht. Die folgenden falschen Verhaltensweisen könnten in Ihrer Behörde verbreitet sein:

- Passwörter offen notieren (Notizzettel)
- Öffnen von Spam-Mails (Übertragung von Schadcode)
- Verwendung von privaten Wechseldatenträgern und mobilen Geräten (Viren)
- Herausgabe von Daten an Dritte (Social Engineering)
- Nichtabschließen von Büros (Diebstahlrisiko)
- Entfernen vom Arbeitsplatz bei geöffneten Anwendungen oder Akten (Datenschutz)
- Die unbefugte Mitnahme von Daten außerhalb des Behördengebäudes.

Für Sie als IT-Sicherheitsbeauftragte/r ist es, wie in den oben beschriebenen Fällen, wichtig, die Beschäftigten auf die mit dem Fehlverhalten einhergehenden Risiken hinzuweisen. Gleichzeitig sollen Sie in dieser Kommunikation auch wertvolle Rückmeldungen zu eventuellen Wissensdefiziten oder Anwendungsproblemen von Ihren Kolleginnen und Kollegen erhalten. Argumentieren Sie deshalb nicht gegen die betroffenen Personen, sondern nehmen Sie eine positive Haltung ein. Etablieren Sie auf diese Weise einen partnerschaftlichen Dialog, der die Beschäftigten zu Verbündeten bei der Durchführung von Informationssicherheitsmaßnahmen macht.

Um im Rahmen der Planungsphase die notwendigen Anknüpfungspunkte für die Inhalte und die Maßnahmenauswahl Ihrer Sensibilisierungsinitiative zu finden, hilft neben der Situationsanalyse (Punkt 1) der Einsatz von anonymen Umfragen. Teilen Sie das Behördenpersonal wenn möglich in Gruppen ein, deren Mitglieder über vergleichbare Kompetenzen bei der IT-Nutzung verfügen und in einem ähnlichen Arbeitsbereich tätig sind — nur so ist eine Vergleichbarkeit gewährleistet. Wählen Sie nun eine (!) Gruppe aus, die entsprechend Ihrer Bestandsaufnahme für die Informationssicherheit von relevanter Bedeutung ist, und lassen Sie von den Mitgliedern anonym einen Fragebogen ausfüllen (Anonymität erhöht die Wahrscheinlichkeit ehrlicher Antworten). Eine Gruppenstärke von rund 10 Prozent der Gesamtbelegschaft reicht in der Regel aus. Um die Qualität der gesammelten Informationen sicher zu stellen, ist es notwendig, dass die Fragen sich vor allem auf die in Punkt 1 definierten Problemfelder beziehen. Außerdem sollten die Fragestellungen nicht in eine vorgegebene Richtung tendieren.

Das Ergebnis der Befragung soll zusammengefasst werden und Ihnen ein Bild von den Erfordernissen und Schwerpunkten für Ihre Sensibilisierungskampagne geben. Darüber hinaus liefert Ihnen der Fragebogen wertvolle Anhaltspunkte zum vorhandenen Wissen und zur Einstellung der Belegschaft.

Tragen Sie die Zusammenfassung Ihrer Analysen der Behördenleitung vor und stellen Sie dar, wo aus Ihrer Sicht konkreter Handlungsbedarf besteht, welche thematischen Anknüpfungspunkte sich für eine Sensibilisierungsinitiative ergeben und wie Ihre Planung aussieht.

Berücksichtigen Sie bei dieser Gelegenheit auch aktuelle Vorgaben, die von der Behördenleitung in Bezug auf die Informationssicherheit gemacht werden. Die Sensibilisierungsinitiative muss sowohl in die Leitlinie zur Informationssicherheit als auch in das Sicherheitskonzept eingebettet sein.

Denken Sie auch daran, die Personalvertretungen in den Planungsprozess einzubeziehen.

3) Ressourcen

Die Entwicklung Ihres Konzepts muss vor dem Hintergrund der verfügbaren Ressourcen geschehen. Bevor Sie mit der Maßnahmenplanung beginnen, sollten daher folgende Fragen in Abstimmung mit der Behördenleitung geklärt sein:

- Welche finanziellen Mittel werden gebraucht und welche Mittel stehen für die Durchführung bereit?
- Wie viel Zeit nehmen die Veranstaltungen oder die anderen Maßnahmen der Kampagne in Anspruch?
- Welche Räumlichkeiten werden gebraucht und welche stehen für eventuelle Veranstaltungen zur Verfügung?
- Gibt es Möglichkeiten der Nutzung von internen Kommunikationsmedien wie Intranet, Newsletter und so weiter (usw.)?
- Welche Beschäftigten können in welchem Umfang zur Unterstützung des IT-Sicherheitsteams herangezogen werden, etwa die Pressestelle oder die Intranet-Redaktion?
- Ist die Einbeziehung von externen Fachleuten möglich?

Nutzen Sie die „Sicher gewinnt! - Die Moderationskarten“, um die Ziele und Themen, Zielgruppen und Kommunikationskanäle zu bestimmen. Damit haben Sie für die weitere Planung eine wichtige Voraussetzung hergestellt.

3.2. Vorbereitung (Phase II)

Das Herzstück Ihres Konzepts zur Durchführung einer Sensibilisierungsinitiative ist der konzeptionelle Aufbau und die strategische Planung. Reflektieren Sie zu Beginn Ihrer Überlegungen die Rollen der Beschäftigten. Fragen Sie sich: Welche Pflichten und Aufgaben haben diese innerhalb Ihrer Behörde und wie können sie für eine positive Auseinandersetzung mit dem Thema Informationssicherheit gewonnen werden? Wie können sie weiter für einen sensiblen Umgang mit Daten und Informationstechnik motiviert werden?

Beachten Sie dabei, dass es wenig Erfolg versprechend ist, bei den Beschäftigten durch Zwänge oder Überredungskünste ein Bewusstsein für die Notwendigkeit von Informationssicherheit zu bilden.

1) Die Elemente Wissen, Handlungskompetenz und Motivation

IT-Sicherheitsbeauftragte müssen durch Kommunikation überzeugen. Drei zentrale Elemente sollten Ihre Vorgehensweise prägen:

- Wissen durch Information: Verzichten Sie auf Belehrungen und liefern Sie stattdessen Informationen und Techniken, mit denen sich die Beschäftigten erfolgreich Wissen aneignen können. Bringen Sie dabei möglichst alltagstaugliche Beispiele zur Veranschaulichung. Dieses Wissen ist die Voraussetzung dafür, dass die Belegschaft für den Zusammenhang zwischen eigenem Handeln und möglichen Konsequenzen sensibilisiert wird.
- Handlungskompetenz durch Dialog: Etablieren Sie den partnerschaftlichen Dialog, denn nur die enge Rückkopplung mit den Beschäftigten gibt Ihnen wertvolle Hinweise zu bestehenden Problemen. Außerdem können Sie so schnell auf Fehlentwicklungen reagieren und die Beschäftigten erhalten die Chance, eigene Vorschläge oder Anmerkungen einzubringen.
- Motivation durch Eigenverantwortung: Fördern Sie die Eigenverantwortung der Beschäftigten und unterstützen Sie selbstständiges Engagement. Setzen Sie Anreize zur Auseinandersetzung mit dem Thema, etwa durch Informations- oder Schulungsangebote, und ermutigen Sie sie dazu, gewonnene Kompetenzen auch einzusetzen und anderen bei Bedarf zu helfen. Kommunizieren Sie positive Entwicklungen, denn Lob und Erfolgserlebnisse steigern die Bereitschaft, das eigene Verhalten zu verbessern.

Verstehen Sie die oben genannten Elemente Information, Dialog und Motivation als gleichwertige, zusammengehörige Komponenten. Je besser Sie diese in Ihre Vorgehensweise integrieren, desto größer ist die Wahrscheinlichkeit, dass Sie Ihre Ziele erfolgreich erreichen.

Die ENISA erläutert in ihrer Publikation »Wege zu mehr Bewusstsein für Informationssicherheit« ab Seite 13 anhand von Diagrammen und Prozessbeschreibungen die Planung, Organisation und Durchführung von Sensibilisierungsinitiativen zur Informationssicherheit. Nutzen Sie die vielfältigen Kommunikationskanäle, um Ihre Themen ins Gespräch zu bringen.

Nach diesen grundsätzlichen konzeptionellen Überlegungen kommen wir nun zur Definition der konkreten Ziele, der Zielgruppen und der Themen. Beachten Sie diese Abfolge, um bei der Konzeption Fehler zu vermeiden und zielgerichtet vorzugehen.

2) Ziele

Bei der Zielsetzung geht es darum, den angestrebten Zustand in Ihrer Behörde zu beschreiben. Die Zielsetzung beantwortet also die Frage, was mit der Sensibilisierungsinitiative erreicht werden soll.

Mögliche Ziele einer Sensibilisierungsinitiative sind:

- Aufmerksamkeit für das Thema schaffen
- Die Beschäftigten über generelle Gefahren aufklären
- Bei den Beschäftigten ein Bewusstsein für Informationssicherheit bilden
- Das Verantwortungsgefühl der Beschäftigten für Informationssicherheit steigern
- Voraussetzungen für sicheres Arbeiten schaffen
- Nachhaltige Verhaltensänderungen hinsichtlich des ermittelten Bedarfs erreichen
- Das Thema innerhalb der Behörde »lebendig« halten
- Verständnis für getroffene Sicherheitsmaßnahmen wecken
- Das Sicherheitsmanagement in der Behörde bekannt machen

Beachten Sie dabei, dass durch eine Sensibilisierungskampagne das Bewusstsein der Beschäftigten für Informationssicherheit steigen kann, sich daraus aber keine zwangsläufige Änderung im täglichen Arbeitsverhalten ergeben muss. Eine belastbare Evaluation der Ziele kann nur durch messbare Kennzahlen erfolgen.

Mögliche Kennzahlen zur Evaluierung einer Sensibilisierungsinitiative sind beispielsweise:

- Weniger Virenalarme / weniger Spam
- Geringere Inanspruchnahme der Hotline
- Mehr Abrufe von Informationsangeboten
- Ergebnisse der Kontrollen der Arbeitsplätze durch das Sicherheitsteam

Darüber hinaus können erneute Befragungen Ergebnisse zum Vergleich mit der ursprünglichen Bedarfsermittlung liefern.

3) Zielgruppen

Um die angestrebten Ziele zu erreichen, müssen Sie das Konzept entsprechend der Mitarbeiterstruktur auf Ihre Zielgruppe abstimmen. Der Erfolg von Sensibilisierungsmaßnahmen hängt eng mit der richtigen Ansprache der Beschäftigten zusammen. Es empfiehlt sich, die Planung zu Beginn auf eine möglichst breite Ansprache an das Personal auf allen Ebenen auszurichten, bevor Sie unter Einbeziehung der Führungsebene im weiteren Verlauf der Kampagne das Konzept an die Bedürfnisse spezifischer Personengruppen anpassen.

Spezifische Zielgruppen sind:

- Personalvertretungen
- Beschäftigte mit Personalverantwortung
- Beschäftigte der IT-Abteilungen
- Beschäftigte mit mobilen Arbeitsplätzen
- Beschäftigte in der Verwaltung mit besonderen Zugangsrechten (z.B. Innerer Dienst)
- Beschäftigte mit besonderen Rechten (z. B. Behördenleitung)

4) Botschaften

Mit der Formulierung der Botschaften legen Sie fest, welche Meinung und Überzeugung Ihre Zielgruppe optimalerweise nach Abschluss einer Sensibilisierungsmaßnahme gebildet haben soll.

Mögliche Botschaften der Sensibilisierungsinitiative sind:

- Informationssicherheit ist von elementarer Bedeutung für unsere Behörde
- Unsere Behörde bemüht sich aktiv um das Thema

- In unserer Behörde gibt es sensible Informationen / Daten, die wir schützen wollen
- Der IT-Sicherheitsbeauftragte unterstützt und fördert die Belegschaft
- Informationssicherheit ist ein fortwährender, dynamischer Prozess

Informationssicherheit geht uns alle an! Deswegen wird an jedem einzelnen Arbeitsplatz über den Grad an Informationssicherheit in einer Behörde entschieden.

3.3. Maßnahmenauswahl (Phase III)

Sie haben den Bedarf definiert und die Ziele, Zielgruppen und Botschaften für Ihre Sensibilisierungsinitiative festgelegt? Dann kommen Sie jetzt in die »heiße Phase« des Projekts. Nun müssen Sie die geeigneten Maßnahmen auswählen, mit denen Sie Ihre Botschaften an die Zielgruppe weitergeben wollen. Denken Sie dabei immer daran, dass Ihre wichtigste Aufgabe zunächst sein muss, Aufmerksamkeit für das Thema Informationssicherheit und die spezifischen Bedürfnisse Ihrer Behörde zu wecken. Ein hohes Aktivierungspotenzial haben praktische Beispiele wie aktuelle Meldungen („Trojaner legt Bundesbehörde lahm"), der Hinweis auf einen kurz zurückliegenden Angriff auf das eigene Behördennetzwerk oder das konkrete Fehlverhalten von – selbstverständlich vollständig anonymisierten – Beschäftigten.

Um die Bediensteten Ihrer Behörde wirkungsvoll zu erreichen, können Sie zahlreiche unterschiedliche Kommunikationskanäle nutzen. Auf Seite 32 ihrer Publikation »Wege zu mehr Bewusstsein für Informationssicherheit« hat die ENISA verschiedene Möglichkeiten aufgelistet.

Für welche Maßnahme oder welches Maßnahmenbündel Sie sich auch entscheiden: Nutzen Sie die gewonnene Aufmerksamkeit, um die Ernsthaftigkeit und die Relevanz des Themas klar zu machen. Sorgen Sie dafür, dass die Beschäftigten erkennen, welchen Beitrag zur Informationssicherheit sie an ihrem Arbeitsplatz leisten können. Folgende Maßnahmen stellt Ihnen dieser Leitfaden zur Verfügung:

1) Einführungs- und Informationsveranstaltungen

Sie gewinnen so viele Beschäftigte wie möglich für die Teilnahme an einer Einführungs- oder Informationsveranstaltung. Sie stellen die Sensibilisierungsinitiative, ihre Ziele sowie die allgemeine Relevanz des Themas in einem Vortrag oder etwa einer PowerPoint-Präsentation vor. Sie geben beispielsweise Hinweise zum richtigen Verhalten und haben die Möglichkeit, zu individuell bestimmten Schwerpunkten externe Fachleute einzubinden. Die Veranstaltung integriert die Teilnehmer durch eine anschließende Diskussion oder Fragerunde.
Mehr zur Durchführung einer Informationsveranstaltung in Kapitel 3.4

2) Workshops

Sie veranstalten für eine kleine Gruppe von Beschäftigten (Vorschlag: maximal 10-12 Personen) einen Workshop. Der Workshop hat den Vorteil, dass in Übungen oder Spielformen eine interaktive und gemeinsame Auseinandersetzung der Teilnehmer mit dem Thema Informationssicherheit erfolgen kann und richtiges Verhalten geprobt wird. Sie haben die Möglichkeit,

externe Fachleute einzubinden.
Mehr zur Durchführung eines Workshops sowie den damit verbundenen Vermittlungstechniken finden Sie in Kapitel 3.4

3) Gründung von Informationssicherheitszirkeln zum Erfahrungsaustausch

Auf freiwilliger Basis schließen sich an der Thematik interessierte Beschäftigte aus verschiedenen Abteilungen zusammen und tauschen sich unter Ihrer Leitung zu Problemen im Umgang mit der Informationssicherheit aus. Zusätzlich erhalten die Teilnehmenden aktuelle Informationen zur Thematik und bekommen eventuell die Möglichkeit, das IT-Sicherheitsteam im Rahmen von Aktionen zu unterstützen.

4) Informationsmaterial (Poster, Flyer, Broschüren)

Innerhalb der Behörde wird mit unterschiedlichen Materialien auf die Initiative hingewiesen. Sie haben die Möglichkeit, mit Hilfe der Materialien Veranstaltungsangebote oder Informationsangebote bekannt zu machen.
In Teil II Der Werkzeugkasten wird Ihnen Material zur Initiative »Sicher gewinnt!« zur Verfügung gestellt.

5) Intranet, Newsletter und interne Mails

Verfügen Sie in Ihrer Behörde über ein Intranet, können dort die Initiative und unterschiedliche Inhalte zur Informationssicherheit publik gemacht werden. Eine dort etablierte Rubrik zur Informationssicherheit bietet sich untern anderem (u. a.) für die Ankündigung von Maßnahmen, Veranstaltungen, Umfragen sowie für die Veröffentlichung von aktuellen Informationen an. Auch anonymisierte Vorkommnisse im Haus können über das Intranet kommuniziert werden. Einladungen zu Veranstaltungen oder Terminhinweise lassen sich gut über den internen Mailverkehr direkt an die gewünschten Personen versenden. Ein aktueller Newsletter kann bestimmte Zielgruppen auf dem neusten Kenntnisstand halten, beispielsweise zur Gefahrenlage informieren oder auf sinnvolle Verlinkungen hinweisen.

6) Aushänge

Wenn Ihnen regelmäßig Vorkommnisse auffallen, wo gegen einfache Regeln verstoßen wird, können Sie über Aushänge auf dem Flur, an Türen oder am »schwarzen Brett« auf die Probleme aufmerksam machen. Ein solches »schwarzes Brett« kann auch Bestandteil des Intranets sein.

Bei der Wahl der Maßnahmen sollten Sie die in Kapitel 2 beschriebene dynamische Entwicklung des Sicherheitsprozesses und die Kultur Ihrer Behörde im Auge behalten. Denn um das Thema Informationssicherheit nachhaltig im Bewusstsein der Beschäftigten zu verankern, werden Einzelmaßnahmen kaum ausreichen. Vielmehr ist es Ihre Aufgabe, ein Konzept zum Zusammenspiel unterschiedlicher Maßnahmen auszuarbeiten.

Beispiel für die Maßnahmenabstimmung unter Berücksichtigung der drei Lernstufen Information, Dialog und Motivation:

- Sie beginnen die Umsetzung Ihrer Sensibilisierungsinitiative mit dem Aushang von Materialien, die bei den Beschäftigten Aufmerksamkeit für das Thema weckt. (Information und Dialog)
- Im Rahmen einer Einführungsveranstaltung stellen Sie der Belegschaft die Materialien noch einmal vor und geben zusätzliche Hintergrundinformationen. (Information und Dialog)
- Über eine interne Rundmail weisen Sie zeitnah auf eine neue Rubrik zum Thema Informationssicherheit im Intranet hin. Auf demselben Weg kündigen Sie Veranstaltungen an. In der Mail wird auch darauf hingewiesen, welche Beschäftigten wann und wo geschult werden. (Dialog und Motivation)
- Sie führen für die ausgewählte Zielgruppe einen oder mehrere Workshops durch. (Information, Dialog, Motivation

7) Zeitplan für Maßnahmengestaltung

Damit die Maßnahmen einer Sensibilisierungskampagne nachhaltig Wirkung zeigen, sollten Sie mit realistischen Zeitplänen aufeinander abgestimmt werden. Ein Zeitplan dient als nützliche Orientierungshilfe und muss natürlich den jeweiligen Bedingungen der Behörde angepasst werden.

In Teil II Der Werkzeugkasten finden Sie einen Vorschlag für einen Zeitplan zur Durchführung von Maßnahmen.

3.4. Durchführung (Phase VI)

Um Ihnen die Durchführung der Sensibilisierungskampagne zu erleichtern, wird im Folgenden die Umsetzung der in Kapitel 3.3 vorgestellten Maßnahmen beschrieben. Wählen Sie die Aktionen aus, die für Sie hilfreich sein könnten.

1) Einführungsveranstaltung

Bei der Einführungsveranstaltung geht es darum, die Relevanz des Themas klar zu formulieren und die Zuhörerenden davon zu überzeugen, dass Informationssicherheit bei ihrem persönlichen Verhalten beginnt. Das gilt selbstverständlich auch für alle weiteren Vorträge, beispielsweise vor der Behördenleitung.

Begrüßung

Bereits hier können Sie ein Zeichen setzen, welchen besonderen Stellenwert das Thema Informationssicherheit für Ihre Behörde hat. Sorgen Sie deshalb wenn möglich dafür, dass die Behördenleitung anwesend ist und die Anwesenden zu Beginn der Veranstaltung willkommen heißt.

Vorbereitung eines Vortrags

Als zentrales Element der Einführungsveranstaltung eignet sich ein Vortrag, in dessen Verlauf auch die Initiative und die geplanten Maßnahmen vorgestellt werden sollen. Wichtig: Der Vortrag darf in keinem Fall zu lang sein und muss inhaltlich lebendig gestaltet werden, weil sonst die Aufmerksamkeit der Anwesenden nicht gewährleistet ist. Gliedern Sie die Vorbereitungsphase für einen Vortrag in vier Schritte:

- Ideen sammeln: Definition aktueller Anknüpfungspunkte und Beispiele, die sich dazu eignen, Aufmerksamkeit bei den Zuhörenden zu erzeugen.
- Ziel definieren: Bestimmung der Inhalte, die kommuniziert werden sollen. Dabei muss auch beachtet werden, wer die Informationen erhalten soll und in welcher Reihenfolge dies sinnvollerweise geschieht.
- Ausarbeiten: Formulieren Sie Ihren Vortrag nicht Wort für Wort aus, sondern arbeiten Sie mit Stichworten, präsentiert mit PowerPoint oder vergleichbaren OpenOffice-Programmen.
- Üben: Wenn Sie wenig Erfahrung im Halten von Vorträgen haben, sollten Sie den Vortrag entweder alleine oder vor ausgewählten Testpersonen üben. Das verschafft Ihnen zusätzliche Sicherheit.

Halten eines Vortrags

Beim Halten eines Vortrages geht es nicht nur um die vermittelten Inhalte. Mit Ihrer Stimme, Ihrer Mimik und Gestik senden Sie weitere Signale an die Zuhörenden aus. Hier die wichtigsten Regeln, die Sie beim Sprechen beachten sollten:

- Halten Sie den Blickkontakt zu den Anwesenden!
- Vermeiden Sie zu viele Nebensätze!
- Sprechen Sie frei und möglichst in Hauptsätzen!
- Eine positive Gestik und Mimik (Lächeln, Humor im Vortrag, keine stocksteife Körperhaltung) verbessern die Wirkung Ihres Vortrages!

Abschluss des Vortrags
Der letzte Punkt Ihres Vortrags sollte eine Aufforderung zum Handeln enthalten. Teilen Sie den Anwesenden mit, wie sie sich über diese Kampagne informieren und selbst einbringen können. Planen Sie unbedingt Zeit ein, um im Anschluss an Ihren Vortrag Fragen zu beantworten und Anregungen aufzunehmen.

Suchen Sie sich ggf. eine Person, die Sie organisatorisch unterstützt, Fragen aus dem Auditorium aufnimmt sowie auf das Zeit-management achtet.

Formale Tipps für eine PowerPoint-Präsentation oder die Foliengestaltung:
- Nutzen Sie die Logos Ihrer Behörde und das »Stempel-Logo« der Kampagne für die Gestaltung Ihrer Folien.

Weitere Informationen zum »Stempel-Logo« finden Sie Teil II Der Werkzeugkasten
- Überladen Sie die Folien nicht mit Text: Verzichten Sie auf ausformulierte Sätze und verwenden Sie stattdessen möglichst kurze Stichworte und Aufzählungen.
- Achten Sie darauf, dass auch Personen, die etwas weiter entfernt sitzen, die Schrift gut lesen können.

Im WERKZEUGKASTEN (ONLINE) finden Sie eine Masterfolie, die Sie an Ihre Behörde anpassen können.

Evaluation
Sowohl Einführungsvorträge als auch Workshops (siehe 2.) sollten Sie nachbereiten. Das Ziel ist, die Reaktionen aus der Behörde auf Ihre Aktivitäten zu erfassen und die Planung Ihrer Kampagne im Detail an den neuen Sachstand anzupassen. Wichtig ist dabei, eine gute Mischung zwischen permanenten Instrumenten zur Sensibilisierung (Plakate, Newsletter, Intranet…) und punktuellen Aktionen (Vorträge, Workshops, »Informationssicherheitszirkel«) zu finden.
Stimmen Sie Ihre Ideen mit der Behördenleitung ab und setzen Sie sie möglichst zeitnah um.
Mehr dazu finden Sie im Kapitel 3.6

2) Workshop

Der Workshop ist eine Lehrveranstaltung, bei der kleine Mitarbeitergruppen zum Thema Informationssicherheit geschult und trainiert werden. Als interaktives Element vermittelt der Workshop Mitarbeiterinnen und Mitarbeitern außerdem, dass Sie ihre Anregungen ernst nehmen und sie von Anfang an mit einbinden.

Der Einsatz externer Coaches im Rahmen eines Workshops kann sehr sinnvoll sein, da diese in der Regel über umfangreiche methodische Erfahrungen verfügen.
Mehr dazu finden Sie im Kapitel 3.5

Vermittlungstechniken für die Workshopgestaltung
Wissen wird lebendig durch Geschichten, Erfahrungen, Erlebtes, aber auch durch Humor. Die Lernpsychologie empfiehlt daher, bei der Vermittlung von Wissen den Aufbau eigener Erfahrungen in den Vordergrund zu stellen oder Erlebnisberichte vorzustellen, die wie Geschichten erinnert werden können. Bei der Sensibilisierung für Informationssicherheit empfiehlt sich die Simulation des Alltagsgeschehens: Die Teilnehmenden spielen beispielsweise ihre auf Informationssicherheit bezogenen Tagesabläufe nach. Sie oder eine andere kompetente Person kommentieren das Geschehen und ordnen die Aktionen ein. Gute Erfolge können auch mit

provokativen Techniken erzielt werden, bei denen etwa bewusst danach gefragt wird, wie man seinen Arbeitsplatz möglichst unsicher (!) gestalten könnte und möglichst viele Einfallsschneisen für Gefahren offen lässt. In Rollenspielen könnten sich einzelne Beschäftigte in die Position von »Bösewichten« begeben, die dem Unternehmen oder einzelnen Personen schaden wollen.

In Erinnerung bleiben den Teilnehmenden auch oft solche Seminarelemente, die das Kind im Menschen ansprechen: Ein Arbeitszimmer und der elektronische Arbeitsplatz darin wird bewusst mit einigen Gefahren präpariert (etwa: an den PC angeschlossene Digitalkamera oder USB-Sticks, Passwörter auf Notizzetteln am Bildschirmrand). Die Teilnehmenden betreten den Raum nacheinander und versuchen, alle Risiken zu finden. Für gute Stimmung kann auch ein Quiz sorgen: Teilnehmende bekommen reale, aber absurd erscheinende Beispiele von Sicherheitsproblemen gemeinsam mit erfundenen Problemen in Form von Zeitungsschlagzeilen vorgelegt und diskutieren in Kleingruppen über deren Echtheit. Damit sollen nicht unbedingt konkrete Gefahren im Arbeitsalltag aufgezeigt werden. Es geht darum, auf die Kreativität der Angreifenden hinzuweisen.

Beispiele für Schlagzeilen: „Forscher arbeiten an Hacker-sicherem Herzschrittmacher“ (echt!) oder „Manipulierte Notizblöcke übermitteln Passwörter an Kriminelle“ (falsch!).

Bei der Gestaltung derartiger Spiele sind der Kreativität keine Grenzen gesetzt. Wichtig ist allerdings, dass der dadurch vermittelte Wissensaspekt im Anschluss auch nochmals zur Sprache kommt – sonst bleibt der Eindruck hängen, dass allein das spielerische Element im Vordergrund stand. Daneben kann aber natürlich auch auf klassischere Techniken zurückgegriffen werden, wie etwa Multiple Choice Tests zu Sicherheitsfragen und die nachfolgende Diskussion der individuellen Antworten. Ausreichend Raum sollte auch für die Schilderung eigener Erlebnisse der Teilnehmenden bleiben.

Hier nochmals die wichtigsten Tipps für Ihre Workshopgestaltung:

- Persönliche Erfahrungen sind für die Teilnehmenden lehrreicher als Frontalvorträge!
- Simulationen, Rollenspiele, Anekdoten und quizartige Elemente mit Alltagsbezug machen Spaß, darüber wird auch nachher noch geredet!
- Lassen Sie Ihrer Kreativität bei der Gestaltung freien Lauf, aber stellen Sie zum Schluss die Punkte, die Sie durch Simulationen usw. vermitteln wollten, nochmal sachlich dar!

Beachten Sie bei der Planung von Workshops auch die in Teil II Der Werkzeugkasten genannten Informationsquellen!

3) Informationssicherheitszirkel

Der Informationssicherheitszirkel ist eine interne Dialogmaßnahme, mit der das Thema Informationssicherheit für die Beschäftigten einer Behörde »lebendig« gehalten werden soll. Für eine Teilnahme empfehlen sich beispielsweise Personen aus verschiedenen Dialoggruppen, die im Rahmen Ihrer Maßnahmendurchführung ein besonderes Interesse am Thema zeigen. IT-Sicherheitsbeauftragte sollten diese Beschäftigten dazu motivieren, sich unter Ihrer Anleitung als Gruppe in regelmäßigen Abständen zu den verschiedenen Aspekten der Informationssicherheit auszutauschen und entsprechende Voraussetzungen dafür schaffen (freier Tagungsraum, Befreiung vom Dienst für die Dauer des Treffens usw.). Der Ablaufplan für ein Treffen des Informationssicherheitszirkels könnte so aussehen:

- Begrüßung der Teilnehmenden, anschließend wird eine Person zur Protokollierung bestimmt. Sollten außenstehende Gäste (z.B. Beratungsunternehmen) teilnehmen, werden diese der Runde vorgestellt.
- Vortrag zu einem aktuellen Aspekt der Informationssicherheit.
- Diskussion des Vortrags. Sie bringen Anknüpfungspunkte zur behördeninternen Arbeitssituation ein.
- Die Teilnehmenden des Sicherheitszirkels erfahren in der Diskussion Details zu den Hintergründen und Plänen zur Informationssicherheit in Ihrer Behörde. Sie erhalten damit ein Bonus-Wissen, das auch eine Motivation zur weiteren Teilnahme am Sicherheitszirkel darstellt.
- Aus den besprochenen Inhalten leiten sich ggf. Aufgaben für bestimmte Personen des Sicherheitszirkels ab oder die Weitergabe von Informationen an die anderen Beschäftigten einer Abteilung bzw. eines Referats. Die protokollierende Person muss die Aufgabenverteilung festhalten und Ihnen eine Zusammenfassung der besprochenen Fakten zukommen lassen. Dadurch können Sie bei der nächsten Sitzung auf bestimmte Inhalte erneut eingehen und Ergebnisse abfragen.

4) Newsletter

Ein Informationssicherheits-Newsletter kann ein wichtiges Medium darstellen, um das Thema bei allen Beschäftigten präsent zu halten. Die Meldungen sollten kurz und knapp gehalten und Fachbegriffe weitgehend vermieden werden.
Sie können Ihren Newsletter aber auch z.B. mit Meldungen aus dem Newsletter des BSI (z. B. www.buerger-cert.de) anreichern.

5) Intranet

Machen Sie die Termine und Nachrichten zur Informationssicherheitskampagne für alle im Intranet verfügbar und nutzen Sie bei der Gestaltung von Inhalten die Materialien von Teil II Der Werkzeugkasten. Fordern Sie die Beschäftigten auf, sich über das Intranet via E-Mail mit Ihnen in Verbindung zu setzen, wenn sie Fragen und Anregungen zum Thema haben oder Beobachtungen an ihrem Arbeitsplatz gemacht haben, von denen Sie wissen sollten.

3.5. Einbindung Externer

Wenn es um die didaktische Vermittlung von Fachwissen in Ihrer Behörde geht, sollten Sie den Einsatz externer Fachleute aus dem Bereich Moderation, Seminargestaltung und Informationssicherheit in Betracht ziehen. Diese sind speziell dafür ausgebildet, Probleme zu veranschaulichen und direkt auf Reaktionen von Teilnehmenden einzugehen. Sie verstehen es, mit Widersprüchen, anfänglichem Desinteresse oder Blockadehaltungen von Teilnehmenden umzugehen, Diskussionen in Fluss zu bringen und ergebnisorientiert zu führen. Darüber hinaus können innerbehördlich kontroverse, sensible Themen zur Informationssicherheit durch Externe leichter angesprochen werden. Wenn Sie sich also nicht ganz sicher sind, ob Sie z. B. eine Einführungsveranstaltung erfolgreich strukturieren und moderieren können, kommt hier der Einsatz von externen Coaches in Frage.
Im Rahmen des Vergabeverfahrens sollten Sie auf zwei Punkte achten: Die formale Qualifikation kann durch Zertifikate belegt werden, über deren Aussagekraft Sie sich bei einschlägigen Einrichtungen wie dem Deutschen Institut für

Erwachsenenbildung oder der Deutschen Gesellschaft für Supervision informieren können. *Passende Weblinks finden Sie als Informationsquellen in Teil II Der Werkezugkasten*

Beachten Sie bei den Vergabegesprächen auch die menschliche Komponente: Ist das eine Person, die zu meiner Behörde und zu meinen Kolleginnen und Kollegen passt? Buchen Sie keine externen Fachleute, ohne sich vorher in einem Gespräch oder einem Probevortrag einen persönlichen Eindruck verschafft zu haben.

Ein externer Coach ist auf ein umfassendes Briefing durch das Sicherheitsteam angewiesen. Ohne grundsätzliche Informationen zu Ihrer Initiative sowie Ihren Zielen und Botschaften kann das Beratungsangebot nicht auf Ihre Bedürfnisse abgestimmt werden.

Für und gegen die Einbeziehung Externer sprechen verschiedene Argumente. In Folge eine Übersicht:

Pro
+ nachgewiesene didaktische Kompetenz
+ manchmal anerkannter als Interne (»Propheten im eigenen Lande«)
+ haben Erfahrung im Strukturieren ergebnisorientierter Veranstaltungen
+ können als Außenstehende innerbetrieblich heikle Themen einfacher ansprechen

Contra
- Kosten
- zeitaufwendiger Auswahlprozess, fachliche Kompetenz und persönliche Eignung müssen überprüft werden
- nicht sinnvoll, wenn die Fragestellung so betriebsspezifisch ist, dass sich Externe extrem lang einarbeiten müssten

Checkliste wichtiger Punkte bei der Auswahl externer Fachleute:

- Formale Qualifikation (Zertifikate, Referenzen, Verbandsmitgliedschaften)
- Kostenrahmen
- Persönlicher Eindruck (Kriterien setzen wie z. B. menschliche Überzeugungskraft, passende Ansprache für die Zielgruppe)
- Fundierte Kenntnisse im Bereich Informationssicherheit. Manchmal ist jedoch ein unbefangener Zugang hilfreicher.
- Verfügbarkeit zu den Wunschterminen bzw. Bereitstellen von Ersatz-Coaches

3.6. Evaluation (Phase 5)

Evaluation ist die systematische Untersuchung des Nutzens oder Wertes eines Gegenstandes. Mit dem Begriff »Evaluation« ist also eine kritische Bewertung des Erfolgs oder Misserfolgs einzelner Aktionen und der Sensibilisierungskampagne insgesamt gemeint.

Die Bewertung sollte auf drei Ebenen erfolgen:

1) Ebene der Teilnehmenden

Die Teilnehmenden von Veranstaltungen, die im Rahmen der Sicherheitskampagne durchgeführt werden, sollten als Feedback einen Fragebogen ausfüllen.

2) Ebene der IT-Sicherheitsbeauftragten

Sinnvolle Wünsche und Anregungen aus

den Fragebögen sollten Sie in Ihrer weiteren Arbeit aufgreifen. Generell sollten Sie für sich in regelmäßigen Abständen (z. B. in Vorbereitung auf Meetings mit der Behördenleitung, in der das weitere Vorgehen abgestimmt wird) auch selbst einige Fragen stellen:

- Bin ich mit der Sensibilisierungskampagne auf dem richtigen Weg? Welche Reaktionen erhalte ich?
- Welches Image hat die Sensibilisierungskampagne bei den Beschäftigten? Sind die richtigen Zielgruppen, Themen und Kommunikationskanäle gewählt worden? Stimmt der Zeitpunkt? Erreiche ich die Beschäftigten?
- Hat die Kampagne zu nachprüfbaren Verhaltensänderungen geführt? Trage ich zur Souveränität der Beschäftigten im Umgang mit elektronisch gespeicherten Texten und Daten bei?
- Stehen Aufwand und Wirkung in einem ausgeglichenen Verhältnis? Ist die Kampagne effizient?
- Sind die Wirkungen der Kampagne von Dauer? Ist die Kampagne nachhaltig? Haben wir die Ziele der Kampagne erreicht?

Sie finden ein Muster für einen solchen Evaluierungsfragebogen, der Ihnen helfen soll, wichtige Rückmeldungen zu Ihrer Kampagne zu erhalten, auf Seite 23.

Überlegen Sie, in welchen dieser Punkte Ihre Kampagne optimiert werden müsste und mit welchen Mitteln dies geschehen könnte. Führen Sie diese Evaluation nicht erst dann durch, wenn die Situation verfahren ist und die Missstimmung wächst. Mindestens ein Mal im Jahr (im ersten Jahr sicher häufiger) machen solche Evaluationen Sinn.

Am besten führen Sie die Evaluation in einer kleinen Gruppe von ständig an der Kampagne beteiligten Personen durch, damit sich die Eindrücke gegenseitig ergänzen.

3) Ebene der Behördenleitung

Erstatten Sie der Behördenleitung über die von Ihnen durchgeführten Maßnahmen Bericht und präsentieren Sie die Ergebnisse Ihrer Evaluation. Auf Basis dieser Ergebnisse kann die Behördenleitung die bisherigen Fortschritte bewerten, des Weiteren erhalten Ihre Vorgesetzten ein umfassendes Bild von den aktuellen Erfordernissen der Sensibilisierung.

Zusammengefasst erfolgt die Feinjustierung Ihrer Sensibilisierungsinitiative also über fünf Elemente:

- Ihr persönlicher subjektiver Eindruck bzw. der Eindruck des gesamten IT-Teams
- Das Ergebnis der Fragebögen
- Die Ergebnisse von Workshops
- Das Ergebnis Ihrer Evaluation aufgrund der fünf oben genannten Fragen zur Wirksamkeit der Kampagne
- Die Einbeziehung der Behördenleitung

Berichten Sie Ihrer Behördenleitung über die Ergebnisse und das weitere Vorgehen. Geben Sie, wenn erforderlich, Informationen zum Beispiel an die IT-Abteilung weiter.

Fragebogen zur Veranstaltung im Rahmen von "Sicher gewinnt!"

Wir freuen uns, dass Sie im Rahmen der Sensibilisierungsinitiative "Sicher gewinnt!" an dieser Veranstaltung teilgenommen haben. Wir wollen unser Angebot weiter optimieren. Dafür brauchen wir Ihre Anregungen und Ihre Kritik. Vielen Dank!

Bitte bewerten Sie die Organisation der Veranstaltung

Ablauf der Veranstaltung:

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Eignung und Ausstattung des Veranstaltungsorts

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Organisation im Vorfeld

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Bitte bewerten Sie die Inhalte der Veranstaltung

Qualität der Themenauswahl und der präsentierten Inhalte

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Nutzen der Inhalte für meine Arbeit

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Bitte bewerten Sie die Didaktik der Veranstaltung

Qualität und Verständlichkeit der Vortragenden

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Wie hat Ihnen die Veranstaltung insgesamt gefallen?

Gesamteindruck

❒ sehr gut ❒ gut ❒ mäßig ❒ ungenügend

Welche Veranstaltungen oder Themen aus dem Bereich der Informationstechnik würden Sie gern vertiefen?

_____

_____

Hier ist Raum für Anmerkungen, Lob, Kritik oder Hinweise:

_____

_____

_____

Impressum

Bundesakademie für öffentliche Verwaltung
im Bundesministerium des Innern
– Lehrgruppe 5 –
Willy-Brandt-Str. 1
50321 Brühl

Tel.: 0228/99 629 - 0
E-Mail: sibe-lg5@bakoev.de

Gestaltung

K_2G - die Kommunikationsagentur
Wikingerufer 7
10555 Berlin

www.k2g.de

Bildnachweise

Titelbild: Fotolia

Stand: Juni 2011