Bundesministerium des Innern, für Bau und Heimat

BAköV

Abbildung 1 aboutpixel.de: Ronald Leine

Sensibilisierung für die Informationssicherheit und den Datenschutz in der öffentlichen Verwaltung

03/2021

Sensibilisierung für die Informationssicherheit und den Datenschutz in der öffentlichen Verwaltung

Der Leitfaden

Bundesakademie für öffentliche Verwaltung
www.bakoev.bund.de

Inhaltsverzeichnis

1. Über den Leitfaden

Bereits in der Basis-Absicherung nach BSI-Grundschutz wird im Baustein ORP.3 die Sensibilisierung der Institutionsleitung und die Einweisung des Personals in den sicheren Umgang mit IT als MUSS-Anforderung definiert. Auch der UP Bund 2017 enthält Awarenessvorgaben für die Bundesverwaltung. Im Bereich des Datenschutz folgen Obliegenheiten zur Sensibilisierung aus der EU-DSGVO.

Somit ist Informationssicherheit und Datenschutz während der Arbeit ein wichtiges Bildungsziel von Schulungs- und Awareness-Maßnahmen. Dabei sollte der Privatbe-reich immer mit einbezogen werden. Bei der Planung und Umsetzung von Awaren-ess-Maßnahmen stellen sich mehrere Herausforderungen. Dieser Leitfaden dient IT-Sicherheitsbeauftragten – aber auch Datenschutzbeauftragten, dem administrati-ven/operativen Datenschutz oder Geheimschutzbeauftragten – bei der Realisierung entsprechender Maßnahmen als praktische Arbeitshilfe – beispielweise zu folgenden Fragen:

- Wie geht man heran?
- Wie definiert man die Themen?
- Wen will man erreichen?
- Warum sensibilisieren wir?
- Wie genau wird der Ablauf geplant?
- An welcher Stelle ist der Einsatz welcher Materialien sinnvoll?
- Wie ist vorzugehen, wenn nur eine Führungskräfteschulung durchgeführt werden soll?
- Welches Maß an Informationen und Maßnahmen ist angemessen und führt nicht zur De-Sensibilisierung?

Der Werkzeugkasten und eine Vielzahl von Materialien im Werkzeugkasten wurden 2021 aktualisiert. Die Instrumente sind online in der jeweiligen aktuellen Version unter https://lernplattform.intranet.bund.de im Fortbildungsportal verfügbar.

1.1 Erläuterung der Symbole

Besonders nützliche Inhalte werden durch vier verschiedene Symbole hervorgehoben:

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

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

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

Das Icon „Werkzeugkasten“ (Symbol Werkzeugkasten) sagt Ihnen, dass Sie die dargestellten Kommunikationsinstrumente online im Werkzeugkasten finden.

1.2 Grundlage des Leitfadens

Der vorliegende Leitfaden ist Teil der Kampagne „Sicher gewinnt!“ der BAköV. Er enthält Instrumente für Planung, Durchführung und Evaluation von Sensibilisierungs-Maßnahmen.

Die Inhalte des Leitfadens und des Werkzeugkastens wurden den aktuellen Bedingungen und Materialien der Sicherheitskampagne „Sicher gewinnt!“ angepasst und basieren auf einer Vielzahl von Sensibilisierungs-Maßnahmen und Erfahrungen, die auf Bundes- als auch auf Länderebene gemacht wurden. Er wurde von den Beschäftigten der Lerngruppe 5 der Bundesakademie gemeinsam mit Fachleuten, unterrichtenden und beratenden Personen aus Dienstleistungsunternehmen überarbeitet.

1.3 IT-Sicherheitsbeauftragte, behördliche Datenschutzbeauftragte, Geheimschutzbeauftragte

Das Thema Informationssicherheit trifft die Bereiche der Beauftragten sowohl in der IT-Sicherheit wie dem Datenschutz (auch den administrativen/operativen Datenschutz) und dem Geheimschutz. Es bietet sich an, dass die Beauftragten und administrativen/operativen Stellen an dieser Schnittstelle in der Sensibilisierung zur Informationssicherheit und zum Datenschutz zusammenwirken. Sie müssen zusammen, aber mit eigenem Blickwinkel agieren. IT ist essenzieller Bestandteil nahezu aller informationsverarbeitenden Prozesse. Insofern sollten innerhalb einer Maßnahme, die sich gegenseitig beeinflussenden Bereiche verknüpft werden. Bei der Planung von Maßnahmen sollten die genannten und andere betroffene Bereiche daher von Beginn an zusammenspielen. Teile einer Maßnahme werden organisatorische Bereiche beeinflussen, wie zum Beispiel die Neueinstellung von Beschäftigten, um die „Neuen“ direkt bei Eintritt in IT-Sicherheits-, Fehler- und Lernkultur willkommen zu heißen.

Der grundsätzliche konzeptionelle Aufbau einer Maßnahme kann auch von Beauftragten für Datenschutz oder Geheimschutz verwendet werden. Ein solcher Prozess zur Sensibilisierung kann gleichermaßen in den Bereichen IT-Sicherheit, Datenschutz oder Geheimschutz umgesetzt werden. Dabei solle darauf geachtet werden, dass es nicht zu einer Überfrachtung von Themen und Maßnahmen kommt. Ein gemeinsam abgestimmtes Vorgehen unterstützt wesentlich den Erfolg solcher Maßnahmen.

2. Awareness braucht Ideen & unterstützende Personen – Grundlagen und Rahmenbedingungen einer Awareness-Kampagne

Die aktuellen und künftigen Herausforderungen für die Informationssicherheit in der öffentlichen Verwaltung sind groß: Mit der umfangreichen Digitalisierung der Verwaltung und der technologischen Entwicklung gehen eine immer stärkere Vernetzung und steigende Komplexität von IT-Systemen einher. Die aktuelle Gefährdungslage für die IT bleibt hinsichtlich des zu verzeichnenden Angriffspotenzials kritisch.

Der Faktor Mensch wurde bei der Gefahrenabwehr oft vernachlässigt. Dabei zeigen die bereits durchgeführten Awareness-Kampagnen immer wieder, dass die Qualität der Informationssicherheit an jedem einzelnen Arbeitsplatz entschieden wird. Viele Studien zeigen, dass z.B. Social Engineering Angriffe sich in den vergangenen Jahren verstärkt haben.

Für die Gewährleistung der Sicherheit der Daten und Informationen in der Behörde, ist ein entsprechendes Sicherheitsbewusstsein bei allen Beschäftigten notwendig. Awareness muss ein Bestandteil des Sicherheitsprozesses sein, damit die Behörde ihre Aufgaben sicher und effizient wahrnehmen kann. IT-Sicherheitsbeauftragte, behördliche Datenschutzbeauftragte, operativer/administrativer Datenschutz und Geheimschutzbeauftragte müssen zur Umsetzung ihrer Aufgaben die Sensibilisierung und Schulung der Beschäftigten realisieren. Der vorliegende Leitfaden und die damit verbundenen Instrumente sollen Unterstützung geben.

Denn genau hier setzen Sensibilisierungs-Kampagnen an. Mittels motivierender und anleitender Maßnahmen sollen die Beschäftigten befähigt werden, sensibel und sicher mit den ihnen anvertrauten Daten und der Informationstechnik umzugehen sowie Regeln und Richtlinien zu verstehen und zu akzeptieren. Gleichzeitig sollen die Maßnahmen befähigen, Gefährdungen frühzeitig zu erkennen, entsprechend zu handeln und z.B. an das IT-Sicherheitsteam zu melden.

Es geht um Awareness im Bereich der Informationssicherheit, die Können, Wissen und Wollen bei den Beschäftigten vereint. Das bedeutet innerhalb der Behörde, das sicherheitskonforme Handeln zu ermöglichen, Sicherheit im Umgang mit Problemen zu geben und Einzelne zu motivieren, dies zu tun.

2.1 Rahmenbedingungen

Bei der Planung und Umsetzung von Sensibilisierungs-Maßnahmen gelten folgende Rahmenbedingungen.

2.1.1 Jede Organisation ist einzigartig in ihrer gelebten Kultur – Awareness-Kampagnen sind nur eingeschränkt standardisiert durchführbar

Eine Sensibilisierungs-Maßnahme ist nur selten standardisiert durchführbar, orientiert sich an Aufgaben, an der Fehler- und Lernkultur, der Situation und den Bedingungen in der jeweiligen Behörde. Die Durchführung hängt davon ab, welche Ziele erreicht werden sollen. Rahmenbedingungen wie

z. B. finanzielle und personelle Ausstattung und Dauer üben auf die Ausgestaltung einen starken Einfluss aus. Die Anpassungen an die jeweilige Behörde sind erforderlich, damit sich alle Beschäftigten angesprochen fühlen.

2.1.2 Awareness lebt von Nachhaltigkeit – Awareness-Kampagnen brauchen einen kontinuierlichen Prozess

Sensibilisierung für Informationssicherheit ist ein Prozess, welcher der ständigen Erneuerung bedarf und in die Behördenkultur und Informationssicherheitsmanagementprozesse integriert werden soll. Generell sind regelmäßige, abwechslungsreiche Fortsetzungen oder Wiederholungen (ca. alle 2 Jahre oder anlassbezogen) „bekannter" Aktivitäten notwendig, um den Grad der Sensibilisierung zu erhalten, zu verbessern und neue Beschäftigte einzubeziehen. Dabei sollten nach einer allgemeinen Sensibilisierung für das Thema in der Folge tiefergehende Schwerpunkte anlassbezogen (z. B. weil aktuell bestimmte Phishing-Mails kursieren) sowie geplant aufgenommen werden. Um ein Verständnis für technische Neuerungen zu erwirken, sollte mit deren Einführung eine direkte und auf die Neuerung angepasste Sensibilisierungs-Maßnahme (z. B. Cloud oder Home-Office) einhergehen. Jede Maßnahme bedarf der Vorbereitung und Zielbestimmung sowie einer Evaluation.

2.1.3 Awareness dient dem sicheren Handeln der Beschäftigten – Awareness-Kampagnen wirken übergreifend auf alle Bereiche der Organisation

Sensibilisierungs-Maßnahmen zur Informationssicherheit sind interdisziplinär.

Bei der Planung ist das optimale Zusammenspiel der sich mit dem Thema Informationssicherheit befassenden Beauftragten grundlegend: dazu gehören beispielsweise der Daten- und Geheimschutz, aber auch die Personalabteilung (z.B. zur Etablierung neuer Abläufe bei der Neueinstellung von Beschäftigten). Ein Zusammenwirken mit der Fortbildungsstelle und der Presse- und Öffentlichkeitsarbeit bietet sich an.

Beispielsweise hilft Wissen aus der Psychologie und Werbebranche bei der Beantwortung von Planungsfragen – zum Beispiel „Wie spreche ich Menschen optimal an?" oder „Welche Maßnahmen erreichen welche Wirkung?". Auch sind Wissen über Moderation, didaktische-methodische Kenntnisse und Fähigkeiten erforderlich. Schulungen oder die Einbeziehung externer Fachleute können hier helfen (siehe Kapitel 2.2).

2.1.4 Awareness ist mehr als nur Sensibilisierung – Awareness-Kampagnen können unbewusste Verhaltensmuster aufdecken

Egal ob Social Engineering, Waterholing oder SPAM. Viele Angriffsmethoden machen sich unbewusstes stereotypes Verhalten zu nutze. Das Öffnen eines E-Mail-Anhangs, Beantworten von Fragen am Telefon oder Einstecken eines gefundenen USB-Sticks. Sowohl im gewohnten Alltag als auch in Stress-Situationen können derartige Verhaltensmuster zu Tage treten und für Sicherheitsvorfälle verantwortlich sein. Regelmäßiges Training und eine offene Lern- und Fehlerkultur helfen die Gelegenheiten für Angreifende zu minimieren.

Awareness-Kampagnen können die Beurteilungskompetenz der Beschäftigten erhöhen um im richtigen Augenblick das gewohnt stereotype Verhalten zu unterbrechen und sicherheitsbewusst zu reagieren.

Bei der Vorbereitung und Durchführung von Sensibilisierungs-Maßnahmen sollten IT-Sicherheitsbeauftragte, behördliche Datenschutzbeauftragte und Geheimschutzbeauftragte gemeinsam über Themen und Schwerpunkte beraten. Gegebenenfalls lohnt es sich, die IT-Abteilung und das Notfallmanagement hinzuzuziehen.

Eine Sensibilisierung kann auch dafür genutzt werden, um die gemeinsamen Themen der einzelnen Beauftragten in die eine oder andere Richtung zu vertiefen. Das Thema „Soziale Netze“ könnte beispielsweise vorrangig von dem/der Datenschutzbeauftragten geführt werden. Informationen zum Thema „Umgang mit eingestuften Dokumenten“ könnten durch Hinweise wie „Die/Der Geheimschutzbeauftragte empfiehlt“ ergänzt werden.

2.2 Einbindung externer Fachleute

Mit den durch die BAköV bereitgestellten Materialien und Werkzeugen lassen sich einzelne Maßnahmen, wie Schulungen oder Webseiteninhalte umsetzen. Bei der Realisierung umfangreicher Kampagnen kann es hingegen ratsam sein, Hilfe durch externe Fachleute einzuholen – beispielsweise für die Vermittlung von Fachwissen aus dem Bereich Moderation oder Seminargestaltung oder für die Planung und Umsetzung von Informationssicherheitstagen und langfristigen Kampagnen. Die Wirkung der Maßnahmen steht und fällt mit der Kompetenz, der Vermittlungsfähigkeit der Referierenden und der Zielgenauigkeit der Materialien. Eine falsche Wahl führt schnell dazu, dass das Thema „verbrannt“ wird. Daher sollte die Auswahl durch Prüfkriterien wie z.B. Vorerfahrung, ausgewiesene Fachkompetenz oder eigene Erfahrung vorgenommen werden. Ebenso können Schwerpunkte wie Coaching oder Vortrag gesetzt werden.

Fragen Sie im Kaufhaus des Bundes oder die BAköV nach Rahmenverträgen, die genutzt, oder nach Personen mit Expertise, die empfohlen werden können.

Eine Sensibilisierungskampagne kann nicht komplett an ein Dienstleistungsunternehmen abgegeben werden. Die Anpassung an die Gegebenheiten und Situation der Behörde kann nur durch Sie erfolgen. Nutzen Sie die Kampagne, um die beauftragte Person für IT-Sicherheit, behördlichen Datenschutz oder auch den Geheimschutz bekannt zu machen. Eine Vielzahl von Arbeiten, Abstimmungen und Briefings können nur von den eigenen Mitarbeitenden geleistet werden. Planen Sie also in jedem Falle entsprechend Zeit dafür ein.

2.2.1 Kreativität

Um die Beschäftigten in die Lage zu versetzen, zum Beispiel im Falle eines (möglichen) Angriffes richtig zu reagieren, müssen sie Verständnis für die Informationssicherheit erlangen – etwas, was nicht durch das verpflichtende Lesen der Sicherheitsleitlinie erreicht werden kann. Eine Sensibilisierungs-Kampagne sollte hingegen (in Teilen) wie eine Werbekampagne betrachtet werden: Alle Maßnahmen sollten so ausgelegt sein, dass die Beschäftigten im täglichen Handeln für das Thema eingenommen werden. Entsprechend viel Wert muss auf das äußere Erscheinungsbild der „Kanäle“ (bspw. Plakate oder Flyer) gelegt werden. Die Erfahrung zeigt, dass alle Maßnahmen darauf ausgerichtet sein müssen, jede Person an ihrem Arbeitsplatz mit ihrem individuellen Aufgabenfeld (Zielgruppen definieren) zu erreichen. Die Maßnahmen sollen einen „Mitnahmeeffekt“ haben. Vielfalt in der Ansprache und die Einbeziehungen privater Interessen im sicheren Umgang mit IT sind erfolgsfördernd. Im Folgenden werden ein paar Beispiele für kreative Ansätze gegeben:

2.2.2 Ohne Betroffenheit keine Aufmerksamkeit“ – Der Einstieg

Zu Beginn einer Maßnahme gilt es, die Aufmerksamkeit der Beschäftigten bzw. Zielgruppe zu bekommen. Statt einer einfachen Ankündigung per E-Mail oder Dienstanweisung hilft es hier, durch entsprechende Aktionen die Belegschaft „wach zu rütteln“ und Betroffenheit zu erzeugen (siehe Kapitel 3.2.1). Bei allen Aktionen ist es wichtig, dass die Anwendenden Informationssicherheit als positiv und nützlich begreifen. Nur so kann das Thema innerhalb Ihrer Behörde lebendig bleiben und eine positive und nachhaltige Auseinandersetzung der Belegschaft mit dem Thema erreicht werden.

2.2.3 „Think Big“ – Der IT-Sicherheitstag

Ein entsprechend beworbener IT-Sicherheitstag bietet den Beschäftigten die Möglichkeit, sich zentral mit dem Thema Informationssicherheit auseinanderzusetzen. Der IT-Sicherheitstag kann ein ganz eigenes Instrument sein oder aber als eine eigene Maßnahme in Ihre Kampagne integriert werden. Auch als Abschlussveranstaltung einer Kampagne eignet sich der IT-Sicherheitstag sehr gut.

Die Veranstaltung könnte bspw. die folgenden Module enthalten:

- Themenstände wie bei einer Messe: Belegschaft kann sich zu bestimmten Themen informieren. Dabei sind die Stände verständlich und kurzweilig aufgebaut (z. B. Passwort-Cracker).
- Spiele: Informationssicherheit spielerisch erfahren. Die BAköV bietet hierzu auch Spiele an (z. B. Security Arena). Eine Ausleihe ist möglich.
- Vorträge: Vorträge zu aktuellen Themen (Sicherheit in Sozialen Netzen, Kinder sicher im Internet, Sicheres Online-Banking, IOT, Home-Office etc.), die auch private Interessen der Belegschaft abdecken
- Live-Hacking: Auftritt von Live-Hacker Teams verdeutlicht anschaulich die Gefahren im Netz.
- Aktuelle Themen wie „Safer-Password-Day“ oder Europäischer Datenschutztag aufnehmen.
- Saisonale Angebote mit Bezug auf bspw. Weihnachten, Urlaub oder andere Themen einbringen.

Im Fortbildungsportal der BAköV sind ein Konzeptpapier zur Durchführung eines IT-Sicherheitstages sowie Ankündigungsplakate und Referenzbeispiele anderer Behörden verfügbar.

2.2.4 „Steter Tropfen höhlt den Stein“ – Informationssicherheit jeden Tag

Die Aktionen der Sensibilisierungs-Kampagne sollten so gestaltet werden, dass für Einzelne einfache, gut zu merkende und umzusetzende Handlungstipps für jeden Tag ableitbar sind. Kleine Informationshappen (z.B. „IMMER [Windowslogo-Taste] + [L], wenn Sie den Arbeitsplatz verlassen“) sind eingängig und leicht verständlich und damit besser als einmalige, seitenlange Abhandlungen mit viel Hintergrundwissen.

Eine in variablen Abständen abwechslungsreiche Wiederholung bzw. Auffrischung bereits bekannter Themen und Merksätze kann zum Halten des Niveaus der IT-Sicherheit beitragen. Gezielte Sensibilisierungsmaßnahmen über einen längeren Zeitraum verteilt, etablieren das Thema Informationssicherheit dauerhaft als Teil der Organisations-, Sicherheits- und Lernkultur, Abwechslung in den Maßnahmen und in der zeitlichen Dauer helfen gegen Abstumpfen. Zwischen den Maßnahmen sollten Erholungsphasen geschaffen werden, um dann mit einem neuen Thema wieder zu überraschen. Abwechslung bringt Aufmerksamkeit.

Beispiel: Ein Plakat wie „Nicht vergessen: IMMER [Windowslogo-Taste] + [L], wenn Sie den Arbeitsplatz verlassen“ für ca. drei Wochen aufhängen. Der nächste Merksatz wird dann beispielsweise nicht über ein Plakat, sondern über eine Notiz auf dem Windows-Anmeldebildschirm platziert oder hängen Sie vereinzelte Plakate doch mal falsch herum auf.

2.2.5 „Zuhause abholen“ – Der private Bereich

Die Lernbereitschaft und das Interesse an Informationssicherheit (zum Beispiel einen Flyer zu lesen) sind deutlich höher, wenn ein privater Bezug integriert ist. Entsprechend helfen private Beispiele und Tipps „für Zuhause“, die Mitarbeitenden für das Thema zu interessieren. Eine Transferleistung in den dienstlichen Bereich ist bei nahezu allen Themen möglich. Das Thema lässt sich beispielsweise auch gut mit dem Thema Verkehrssicherheit erklären: Beschäftigte sollten sich bewusst sein, dass sie (immer) entsprechend umsichtig fahren müssen, egal ob sie einen Dienstwagen oder Privatwagen fahren.

Üben, üben, üben!

Die Entwicklung einer Kampagne ist ein kreativer Prozess mit vielen unterschiedlichen Aufgaben, manchmal benötigt man Unterstützung.

„Ich bin Siggi! Meine Arbeitsaufgabe besteht darin, eine Kampagne zu entwickeln. Ich habe das noch nicht gemacht und versuche nun einen Weg zu finden, diese Aufgabe zu lösen. Zuerst beginne ich, mir einen Überblick über meine Fähigkeiten zu verschaffen. Es gilt herauszufinden, was ich allein machen und entscheiden kann und bei welchen Tätigkeiten und Entscheidungen ich Hilfe brauche. Dann überlege ich, wie ich mich selbst organisieren kann, denn bei der Entwicklung einer Kampagne ist Planung notwendig.“

Aufgabe 1: Selbsteinschätzung

Prüfen Sie für sich selbst folgende Aussagen und schreiben Ihre Gedanken auf!

1. Das Schreiben eines Konzepts für eine Kampagne fällt mir leicht, weil ich bereits eine genaue Vorstellung von den Bildungszielen, den Stilmitteln und Gestaltungselementen habe.
2. Ich kann allein Texte und Bildskizzen entwerfen oder eine Veranstaltung planen.
3. Ich produziere die Informationsträger selbst oder gebe sie in Auftrag und ich weiß auch schon wo.

Beispiellösung:

„Ich habe ich mir folgende Gedanken gemacht: Ich weiß noch nicht, ob mir das Schreiben eines Konzepts für eine Kampagne leichtfällt, deswegen entscheide ich mich eher dazu, im Team die Aufgaben zu bearbeiten. Vielleicht ist es sinnvoll, wenn ich das Gespräch mit Kollegen und Kolleginnen suche. Texte und Bildskizzen kann ich gut entwerfen, da weiß ich auch schon, wie ich Ideen zusammentrage. Das Thema der Kampagne ist sehr vertraut, deswegen, weiß ich genau, was die Bilder und Texte aussagen sollen. Bei den Gestaltungselementen wie Farben und Formen berate ich mich nochmal mit meiner Chefin, sie weiß, was gut ankommt. Mit der Produktion der Informationsträger habe ich mich noch nie auseinandergesetzt, klar kenne ich online Druckereien, aber am besten frage ich auch hier meine Chefin, wie es sonst im Haus gemacht wird. Eine Veranstaltung muss ich nicht planen."

Aufgabe 2: Selbstorganisation

Prüfen Sie für sich selbst folgende Aussagen und schreiben Ihre Gedanken auf!

- Wie organisiere ich meine Ideenfindung (Ideenbuch, Ankerpunkte schaffen, Gespräche)?
- Wie erfahre ich relevante Merkmale meiner Zielgruppe?
- Wie erfahre ich, welche Gestaltungselemente und Stilmittel passen könnten, angemessen sind (Perspektiven: Zielgruppen, Kosten, Vorgesetzte/Verantwortliche)?
- Wie viel Zeit benötigt meine Konzeptphase, die Prüfphase von Vorgesetzten/Verantwortlichen und die Produktionsphase der Informationsträger?
- Kann ich selbst die Kampagne starten oder benötige ich Unterstützung bei der Verteilung und/oder Anbringung der Informationsträger oder bei Vorträgen/Workshops?

Beispiellösung:

„Ich habe ich mir folgende Gedanken gemacht: Um mir Ankerpunkte zu schaffen, habe ich mir erstmal die Eckdaten der Kampagne aufgeschrieben. Am besten lassen sich diese mit den W-Fragen festhalten, ganz wichtig ist mir immer, dass ich mich daran erinnere, welches Ziel die Kampagne erreichen soll, deswegen habe ich ihr einen unverkennbaren Namen gegeben, den ich immer als Überschrift setze. Wenn ich in meinem Protokoll, das ich parallel führe, reinschreibe, dann halte ich meine Ideen, Entscheidungen und die meiner Mitarbeitenden und Vorgesetzten fest. Damit ich nicht in Zeitnot geraten kann, unterteile ich mir die Kampagne in Phasen und überlege mir, wie lange ich

für welche Aufgabe benötige. Ja, mir ist klar, dass ich beim Kampagnenstart Hilfe brauche, das bespreche ich noch mit meiner Chefin."

3. Awareness ermöglichen? Mit System – Über das Phasenmodell zum Kampagnenfahrplan

Die Planung und Durchführung der Sensibilisierungs-Maßnahme lässt sich in ein aus vier Phasen („Vorbereitung", „Entwicklung Maßnahmenpaket", „Durchführung" und „Evaluation") bestehendes Phasenmodell unterteilen und wie ein Zyklus behandeln, der ständiger Wiederholung bedarf.

3.1 Phase I: Die Vorbereitung

Ziel der Vorbereitung ist eine Analyse der Ausgangssituation, in der folgende Fragen geklärt werden:

1. Wie ist die Situation im Hause,
   1.1 Zu welchen Themen sind wir gefordert?
   1.2 Was sind die konkreten Ziele der Sensibilisierungskampagne?
   1.3 Was sind die messbaren Zielvorgaben?
2. Welche Themen sollen abgedeckt werden?
   2.1 Mit welchem Gewicht?
   2.2 Welche Zielgruppen und welche Kanäle gibt es?
3. Ressourcen
   3. 1 Welche Ressourcen (Budget, Personen, Material) stehen zur Verfügung stehen?
   3.2 Welche Rolle spielt die Struktur der Behörde?
4. Nutzung oder Schaffung einer Marke für Informationssicherheit bzw. die Kampagne.

Am Ende der Vorbereitung sollte sich eine klare Übersicht der Maßnahmen ergeben. Zur Vorbereitung können die „Sicher gewinnt"-Moderationskarten aus dem Werkzeugkoffer unterstützen.

Die frühzeitige Einbindung der Behördenleitung, der beauftragten Person für Datenschutz und Geheimschutz, Korruption, Gleichstellung, interne Kommunikation und der Personalvertretungen (Aufzählung nicht abschließend) ist für einen reibungslosen Ablauf ratsam. Berücksichtigen Sie auch aktuelle Vorgaben der Behördenleitung in Bezug auf Informationssicherheit. Die Sensibilisierungs-Maßnahme muss sowohl in die Leitlinie zur Informationssicherheit als auch in das Sicherheitskonzept eingebettet sein.

3.1.1 Ziele

Der erste Schritt in Phase I ist die Festlegung der Zielstellung – nicht zuletzt, um die Maßnahmen bewertbar zu machen. Die Zielstellung kann langfristig oder auch nur für einen definierten Maßnah-

menzeitraum festgelegt werden, je nachdem ob eine grundsätzliche Erhöhung der Sensibilität oder ein konkretes Problem angegangen werden soll. Bei der Planung sollte auch die aktuelle Gefährdungslage bzw. Vorfälle in Ihrem Hause mit einbezogen werden, um eine entsprechende Themengewichtung vorzunehmen. In den Zielen wird der angestrebte SOLL-Zustand Ihrer Behörde beschrieben.

Mögliche Ziele einer Sensibilisierungs-Kampagne sind:

- Grundsätzlich Aufmerksamkeit und Interesse für das Thema wecken.
- Aufklären über generelle und spezielle Gefahren.
- Fördern der Wahrnehmung der eigenen Verantwortlichkeit.
- Grund- und Praxiswissen mit konkreten Handlungstipps für mehr Sicherheit vermitteln.
- Ein Bewusstsein für Informationssicherheit bilden / Sicherheits-, Fehler- und Lernkultur etablieren.
- Ein höheres Sicherheitsniveau in der Behörde erreichen.
- Verständnis für getroffene Sicherheitsmaßnahmen wecken.
- Das Sicherheitsmanagement in der Behörde bekannt machen.
- Diese Ziele sollten vorab in Bezug auf ihre Evaluierbarkeit geprüft werden.

3.1.2 Aufnahme des IST-Zustands

Nach Festlegung der Zielstellung sollte eine Bestandsaufnahme der spezifischen Ausgangssituation der Behörde im Hinblick auf die Informationssicherheit erstellt werden. Dazu gehören folgende Elemente:

1. IST-Zustand der Sicherheits-, Fehler- und Lernkultur der Institution,
2. Identifizierung der Themen, Zielgruppen und Kanäle sowie Einbeziehung der aktuellen Gefährdungssituation und entsprechende Gewichtung der Themen,
3. Verfügbare bzw. erforderliche personelle, technische und finanzielle Ressourcen.

IST-Zustand der Sicherheitskultur

Im ersten Schritt muss der IST-Zustand der Sicherheits-, Fehler- und Lernkultur im Haus aufgenommen werden. Eine intensive Recherche bzw. Evaluation wird empfohlen, da sich im weiteren Verlauf der Planung aus diesen Feldern die Themen und der Maßnahmenbedarf ableiten lassen. In diesem Zusammenhang lohnt es sich auch, aktuelle Quellen über die Informationssicherheitslage (zum Beispiel Informationen des BSI) zu berücksichtigen. Folgende Fragen sollten u. a. beantwortet und gewichtet werden:

- Welche Maßnahmen wurden bereits in der Vergangenheit durchgeführt, welche Ergebnisse gab es und welche Konsequenzen hat man abgeleitet. Wie war der Erfolg der durchgeführten Maßnahmen?
- In welchen Bereichen werden sensiblen Informationen/Daten in Ihrer Behörde verarbeitet?
- Was sind die größten Sicherheitsprobleme der Behörde für die Informationssicherheit?
- Welche Sicherheitsprobleme sind in jüngster Vergangenheit aufgetaucht? Sind die Probleme auf Fehlverhalten, Irrtümer oder Stressreaktionen von Beschäftigten zurückzuführen? Wenn ja, auf welche?

- Welches Fehlverhalten, gegebenenfalls beabsichtigte oder unbeabsichtigte Handlungen, Stressreaktionen oder Irrtümer haben Sie bei den Beschäftigten am häufigsten wahrgenommen?
- Wie offen ist der Umgang mit Fehlern?
- Gibt es ein Fehlermanagement, wird der offene Umgang gefördert?
- Wie groß sind die Unterschiede in der Kompetenz beim Umgang mit Informationstechnik?
- Werden in naher Zukunft neue technische oder organisatorische Änderungen umgesetzt?
- Stehen neue Aufgaben für die Organisation an.

Damit 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 Teilnehmenden des Sicherheitsteams, Personen aus den Bereichen Datenschutz/Geheimschutz, Leitungspersonen oder von den Personalvertretungen.

Quellen für die Recherche sind beispielsweise:

- Umfragen und Interviews (siehe auch Phase IV, Evaluation),
- Informationen der Hotline (Help Desk). Diese leisten den Beschäftigten bei Schwierigkeiten in Verbindung mit der Informationssicherheit am Telefon »Erste Hilfe« und dokumentieren die jeweiligen Anfragen und den weiteren Umgang mit der Problemstellung innerhalb der Behörde.

Anhand dieser zusätzlichen Informationen können Sie Ihre eigenen Einschätzungen überprüfen und ggf. um weitere wichtige Punkte ergänzen. Im Sinne einer Evaluation kann es sinnvoll sein den IST-Zustand über Umfragen und Interviews zu ermitteln. Diese Maßnahmen bieten sehr gute Grundlagen zur Evaluation.

Im Anhang befinden sich zusätzlich eine Checkliste sowie ein Fragebogen zur Bedarfsermittlung, mit denen eine Bestandsaufnahme in Bezug auf die Standardinhalte zur Informationssicherheit weiter konkretisiert werden kann.

Dokumentieren Sie die Ergebnisse Ihrer Recherche, sie werden am Ende der Kampagne wertvolle Dienste leisten, inwieweit Sie mit Ihren Maßnahmen erfolgreich waren. Möglicherweise ist es sinnvoll, die Meinung entsprechend qualifizierter Kollegen und Kolleginnen einzuholen, etwa von den Teilnehmenden des Sicherheitsteams, Personen aus den Bereichen Datenschutz/Geheimschutz, den Beauftragten, der Leitung oder von den Personalvertretungen. Nutzen Sie die Ergebnisse für die Begründung der Maßnahmen der Sensibilisierung vor der Hausleitung und für die Erfolgsmessung der Maßnahmen.

Ressourcen

Die Entwicklung des Konzepts muss vor dem Hintergrund der verfügbaren Ressourcen geschehen. Bevor mit der Maßnahmenplanung begonnen wird, sollten folgende Fragen in Abstimmung der Behördenleitung vorgetragen werden:

- Welche finanziellen Mittel stehen bereit oder müssen zu welchem Zeitpunkt beantragt werden?
- Welche Beschäftigten können in welchem Umfang zur Unterstützung des IT-Sicherheitsteams herangezogen werden (z.B. die interne Kommunikation, Intranet-Redaktion, Fortbildungsstelle oder der Personalrat)?
- Wie viel Zeit dürfen Beschäftigtenveranstaltungen oder andere Maßnahmen der Kampagne in Anspruch nehmen?
- Welche Räumlichkeiten stehen für eventuelle Veranstaltungen zur Verfügung?
- Welche internen Kommunikationsmedien wie Intranet, Zeitung für Mitarbeitende, Schwarze Bretter, Newsletter, usw. dürfen verwendet werden?
- Dürfen externe Dienstleistende eingebunden werden?
- Gibt es Rahmenverträge, die genutzt werden können?

Denken Sie nach der Kampagne daran, laufende Mittel für weitere Sensibilisierungsmaßnahmen zu beantragen.

Tragen Sie die Zusammenfassung Ihrer Analysen der Behördenleitung vor und stellen Sie dar, wo konkreter Handlungsbedarf besteht, welche thematischen Anknüpfungspunkte sich für eine Sensibilisierungs-Kampagne ergeben und wie Ihre Planung aussieht. Eine Checkliste unterstützt Sie hier bei der konkreten Umsetzung, eine Muster-Kampagne finden Sie im Teil 2 des Leitfadens, ebenso Hinweise zur Planung

3.1.3 Identifizierung der Themen, Zielgruppen und Kommunikationskanäle

Der nächste Schritt der Vorbereitung umfasst die Definition der relevanten Themen, Zielgruppen und die Kanäle, über die die Themen an die Zielgruppen kommuniziert werden.

Je nachdem, welche Maßnahmen geplant werden, wird das Gesamtkonzept aus mehr oder weniger Elementen bestehen.

Nutzen Sie die „Sicher gewinnt! – Die Moderationskarten“, um die Themen, Zielgruppen und Kommunikationskanäle zu bestimmen. Damit haben Sie wichtige Voraussetzungen für die weitere Planung geschaffen.

Die Themen

Die Informationssicherheitsrisiken für ein Haus sind individuell und unterscheiden sich mit hoher Wahrscheinlichkeit von denen anderer Behörden. Welche Themen bei der Planung relevant sind, lässt sich aus den Ergebnissen des Ist-Zustands ableiten. Gab es beispielsweise des Öfteren Vorfälle, die durch infizierte Spam-Mails verursacht wurden? Oder können sich fremde Personen relativ frei und unbeobachtet in Ihren Gebäuden bewegen? Dann gehören die Themen E-Mail und Zutrittsschutz unbedingt auf die Maßnahmenliste. Eine Auswahl möglicher Themen und das gewünschte Verhalten:

- Basissicherheit (Passwörter nicht notieren / Büro abschließen)
- E-Mail-Sicherheit (Mails prüfen / keine Übertragung von Schadsoftware provozieren)
- Verwendung von privaten Wechseldatenträgern und mobilen Geräten (keine Viren / Datensicherheit)
- Unabsichtliche Herausgabe von Daten an Dritte (Social Engineering)
- Datensicherheit (Verlassen des Arbeitsplatzes nur bei geschlossenen Anwendungen oder Akten / keine Mitnahme von Daten außerhalb des Behördengebäudes)
- Verhalten in der Öffentlichkeit (Mithören von Interna durch Dritte vermeiden)

Ebenso gibt es Themen die sich aus Vorhaben sowie den aktuellen Entwicklungen der Gefährdungslage ergeben. Dementsprechend können die Themen gewichtet und priorisiert werden.

Eine gute Hilfestellung bieten die Moderationskarten der BAköV. Sortieren Sie nicht-zutreffende Karten aus und priorisieren die relevanten Karten nach Gefahrenpotenzial und dem höchsten Aufklärungsbedarf.

Die Zielgruppen

Der Erfolg von Sensibilisierungsmaßnahmen hängt eng mit der Auswahl der richtigen Zielgruppen zusammen. Mögliche Zielgruppen sind z.B.:

- Führungskräfte,
- Personalvertretungen,
- Beschäftigte der IT-Abteilungen,
- Beschäftigte mit mobilen Arbeitsplätzen,
- Telearbeitsplätze,
- Beschäftigte mit besonderen Zugangsrechten (z.B. Innerer Dienst),
- Externe Auftragnehmende oder Dienstleistende,
- Auszubildende, Praktikumskräfte, Lehrkräfte im Referendariat,
- Beschäftigte, die nur zeitweise Zugang zu PCs haben,
- Neue Beschäftigte.

Sinnvoll kann es auch sein, die Zielgruppen nach sozialen Eigenschaften in ihrem beruflichen Kontext zu unterscheiden, hierbei hilft die Persona(e) Methode (Kann über den Rahmenvertrag der BAköV beauftragt werden).

Ein exemplarisches Ergebnis könnte sein:

Leitungsverantwortung und Führung: Referats- oder Abteilungsleitung,

- „IT-Technologie vereinfacht unseren Arbeitsalltag, und ich unterstütze mein Team gerne dabei, diese sinnvoll anzuwenden."
- „Technik verändert sich jedoch sehr schnell, sodass es mir nicht immer gelingt, auf dem Laufenden zu bleiben."
- „Ich kann mich auf die Einschätzung meines Teams in der Regel verlassen."
- „Die mediale Präsenz über Gefahren und Risiken macht mich aufmerksam. Ich habe verstanden, dass Regeln wichtig sind — und deren Einhaltung durch die Mitarbeitenden."

Haltung zur IT-Sicherheit: Sehr geringes Risikobewusstsein und auch eher geringes Interesse. „Ich muss ungehindert kommunizieren, für IT-Sicherheit habe ich keine Zeit. Darum kümmert sich das IT-Referat, das hat mein vollstes Vertrauen. Außerdem mache ich digital ja gar nicht viel und was sollte kriminelle Hacker überhaupt an meiner Person interessieren?" Im Dienst von wichtigen Aufgaben fühlt sich die Person berechtigt, hin und wieder Verhaltensregeln zu brechen. Es ist ihr jedoch wichtig, dass die Mitarbeitenden die Regeln zur IT-Sicherheit unbedingt genau befolgen.

Haltung zur Informationssicherheit: Hier ist das Interesse groß und das Risikobewusstsein hoch. „Vertraulichkeit ist Grundlage meiner Arbeit! Besonders schlimm wäre es für mich, wenn Informationen vorzeitig und ungesteuert an die Medien gingen. Informationssicherheit ist mir daher sehr wichtig. Gefahren lauern überall, vor allem auf Seiten der politischen Gegner."

Handlungssicherheit: Die Führungskraft fühlt sich subjektiv sicher, meint Gefahren zu meiden und sich überwiegend regelgerecht zu verhalten. Objektiv betrachtet unterschätzt diese Persona das Ausmaß der eigenen digitalen Aktivitäten (z. B. externe Anwendungen, „Gimmicks", „Schatten-IT") und das damit verbundene Risiko sowie auch die Risiken, die sie mit gelegentlichen Regelbrüchen eingeht.

Die Ansprache der Gruppen kann sich stark voneinander unterscheiden – beispielsweise zwischen der Gruppe der Führungskräfte und der Ansprache der anderen Ebenen.

Die Themenblöcke sollten an den Wissensstand der Zielgruppe anknüpfen. Aus diesem Grund sollten die Zielgruppen entsprechend den Themenblöcken zugeordnet werden. Beispielsweise gilt für die Zielgruppe der IT-Verantwortlichen: Diese Zielgruppe ist sehr technikaffin und meist mit hohen Zugriffsrechten ausgestattet. Ein Themenblock „Umgang mit eingestuften Daten und hohen Zugangsberechtigungen" wäre für diese Zielgruppe passend, aber nicht für die Gruppe „Standard-Nutzende mit PC" sinnvoll.

Bei einer breit aufgestellten Zielgruppe empfiehlt es sich, die Planung zu Beginn mit einer möglichst breiten Ansprache an alle Beschäftigten auszurichten. Erst im späteren Verlauf können dann unter Einbeziehung der Führungsebenen ausgewählte Inhalte an die Bedürfnisse spezifischer Personengruppen angepasst werden. Denken Sie aber auch daran, dass ein Thema für Kolleginnen und Kollegen in Zukunft relevant oder auch privat interessant sein kann, bevor Sie Themen für eine bestimmte Zielgruppe verwerfen.

Nutzen Sie auch hier die „Sicher gewinnt-Moderationskarten“.

Die Kommunikationskanäle

„Kanäle“ sind Informationswege, mit deren Hilfe die gewählten Themen zur empfangenden Person (Zielgruppen) gebracht werden. Die Kommunikationswege können je Thema, Gruppe und Behörde (Behördenkultur, Struktur und Infrastruktur) völlig unterschiedlich sein. Kanäle machen den kreativen Anteil einer Kampagne aus und dem Ideenreichtum sind diesbezüglich kaum Grenzen gesetzt. Typische Kanäle sind zum Beispiel:

- Schulungen „Informationssicherheit und Datenschutz am Arbeitsplatz”,
- Intranet,
- Hauspost,
- Mitarbeitenden-Zeitung,
- E-Mail / Newsletter,
- Plakate und Flyer,
- Hinweistafeln/schwarzes Brett,
- Personalveranstaltungen,
- Teammeetings,
- E-Learnings,
- Lernvideos,
- Webinare,
- Weitere interne Kanäle wie Verbesserungs- oder Fehlermanagement.

Auch hier liefern die „Sicher gewinnt-Moderationskarten“ Hilfe bei der grundsätzlichen Auswahl.

3.1.4 Die Marke Informationssicherheit – Die Botschaft Informationssicherheit

Um verschiedene Maßnahmen inhaltlich zu bündeln, ist es sinnvoll ein Wiedererkennungsmerkmal für Informationssicherheit bzw. für die Sensibilisierungskampagne zu schaffen. Die Beschäftigten verknüpfen das Merkmal im besten Falle positiv mit dem Thema Informationssicherheit.

Das Wiedererkennungsmerkmal kann dabei als Logo, Wort-Bildmarke und/oder als Slogan entwickelt werden, wobei der Slogan jeweils im Vordergrund steht. Eine weitere Möglichkeit ist es, eine Figur in den Mittelpunkt zu stellen (wie „Siggi Sicher“ der „Sicher gewinnt“-Kampagne der BAköV).

Die mit dem Slogan verbreitete Botschaft wird optimaler Weise so gewählt, dass sie die Meinung und Überzeugung der Zielgruppen nach Abschluss der Sensibilisierungsmaßnahmen widerspiegelt. Mögliche Botschaften der Sensibilisierungskampagne sind zum Beispiel:

- Informationssicherheit ist von elementarer Bedeutung für unsere Behörde.
- Unsere Behörde verbessert regelmäßig die Informationssicherheit.
- In unserer Behörde gibt es sensible Informationen / Daten, die wir gemeinsam schützen wollen.
- IT-Sicherheitsbeauftragte unterstützen und fördern die Belegschaft.
- Informationssicherheit ist ein fortwährender, dynamischer Prozess.

Ein Beispiel aus der Kampagne denk x sicher!: „Informationssicherheit betrifft uns alle!“

3.2 Phase II: Entwicklung eines Maßnahmenpaketes

Nach Phase I ist der Bedarf definiert und die Ziele, Zielgruppen und Botschaften der Sicherheitskampagne wurden erfolgreich festgelegt. In Phase II müssen nun die geeigneten Maßnahmen ausgewählt werden, mit denen die Botschaften der Zielgruppe vermittelt werden sollen. Auch die (grobe) Planung des zeitlichen Ablaufs ist Teil dieser Phase. Eine Kampagne deckt im Idealfall die folgenden Bildungsziele ab:

- Über Betroffenheit Bewusstsein (Awareness) schaffen,
- Informationssicherheit lernen,
- Informationssicherheit in den Alltag integrieren.

Im Werkzeugkasten finden sich dazu weitere Anregungen.

3.2.1 Betroffenheit schaffen

Die Aufgabe zu Beginn einer Durchführung ist es, Aufmerksamkeit für das Thema Informationssicherheit und die Bedürfnisse der Behörde zu wecken. Ein hohes Aktivierungspotenzial haben praktische Beispiele aus dem Alltag, der Hinweis auf einen kurz zurückliegenden Angriff auf das eigene Behördennetz oder offensichtliches Fehlverhalten, Irrtümer oder gefährliche Stressreaktionen von Beschäftigten – selbstverständlich vollständig anonymisiert. Betroffenheit kann aber auch durch eigens initiierte Aktionen erzielt werden. Dies sind zum Beispiel:

- E-Learning Formate wie beispielsweise der BAköV-Krimi DenkXsicher bei dem die Beschäftigten über einen längeren Zeitraum einen Cyber-Krimi mitverfolgen und miträtseln können.
- Trick-E-Mail: Versenden einer Trick-E-Mail. Diese E-Mail enthält einen Trick-Link, der auf die behördeneigene Intranetseite führt und dort in positiven Worten erklärt, dass dies auch ein „gefährlicher“ Link hätte sein können. Hinweis: Für diejenigen, die den Trick erkannt haben, sollte die Aktion ebenfalls aufgeklärt werden.
- Social Engineering: eine beauftragte Person versucht sich Zugang zum Gebäude und möglichst vielen Büros oder telefonisch zu Informationen zu verschaffen. Dies kann eine extern beauftragte Firma sein oder z. B. wenig bekannte Beschäftigte.
- Live-Hacking: Sehr effektiv ist auch ein Live-Hacking z.B. als Auftakt-Veranstaltung. Live-Hackings erläutern sehr kurzweilig, aber doch eindringlich die Gefahrenpotenziale. Ein Live-Hacking lässt sich auch gut im Rahmen einer Personalveranstaltung durchführen, um möglichst viele Beschäftigte zu erreichen. Für das Live-Hacking sollten Sie eine geeignete externe Firma beauftragen (z.B. aus dem BAköV-Rahmenvertrag).

Im Werkzeugkasten finden Sie einen kompletten Live Hacking Film, mit dem Sie sich einen Eindruck verschaffen können, wie eine Live Hacking-Show aussehen kann. Ebenso finden sich dort weitere Filmsequenzen zu einzelnen Themen.

Egal für welche Maßnahmen 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 jede/r Einzelne am Arbeitsplatz leisten kann. Und bitte bedenken Sie bei Ihrer Maßnahmenauswahl immer das beschriebene Motto: „Wecken“ – nicht „erschrecken“.

3.2.2 Lernen – Wissen vermitteln

Nachdem das Bewusstsein für Informationssicherheit bei den Beschäftigten „geweckt“ wurde, sollten die Zielgruppen in die Lernphase geführt werden. Dies sollte durch zielgruppenspezifische, konkrete Handlungsempfehlungen für die entsprechenden Situationen geschehen (z. B. „Was ist zu tun, wenn ich eine vermeintliche infizierte E-Mail erhalten habe?“).

Weisen Sie nicht nur auf das Problem hin („Sie müssen ein sicheres Passwort verwenden!“), sondern bieten Sie direkt eine Lösung an („Ein sicheres Passwort kann folgendermaßen gebildet werden: …“).

Für die Lernphase eignen sich auch typische Schulungen. Dies könnten z. B. sein:

- **Präsenzschulungen:** Die Belegschaft wird in Präsenzterminen geschult. Der Lerneffekt durch Präsenzschulungen ist besonders hoch, allerdings ist auf der anderen Seite auch ein erheblicher Aufwand für die Behörde (Abwesenheit vom Arbeitsplatz) notwendig.

Eine Unterstützung der Fortbildungsstelle des Hauses und die Durchführung durch externe Dienstleistungsunternehmen bieten sich an. Diese besitzen eine hohe Kompetenz in Sachen Informationssicherheit sowie didaktisches Einfühlungsvermögen und Erfahrung bei der Durchführung von Schulungsveranstaltungen. Auch hier sind schon zielgruppenspezifische Angebote möglich.

- **Online-Schulungen**: Mit einer Online-Schulung können gezielt einzelne Themengebiete geschult und – sofern gewünscht – direkt im Anschluss „abgefragt" werden. Der Vorteil dieses Lernformates liegt vor allem in der zeit- und ortsunabhängigen Durchführung. Auch Online-Schulungen benötigen Anreize oder eine Verbindlichkeit, weil erfahrungsgemäß die Durchführung von Online-Schulungen von der Belegschaft gern aufgeschoben wird. Bei den Angeboten muss auf Barrierefreiheit geachtet werden.

Workshops mit dem/der IT-Sicherheitsbeauftragten: Auch IT-Sicherheitsbeauftragte können Workshops zum Thema durchführen und die Mitarbeitenden schulen. Dies kann zum Beispiel auch zusammen mit den Beauftragten für Datenschutz und/oder Geheimschutz geschehen. Möglicherweise gibt es bereits Datenschutzschulungen im Hause, an die sich das Thema Informationssicherheit anschließen lässt. Neben der guten Verbreitung ist hier ein weiterer Vorteil, dass der/die IT-Sicherheitsbeauftragte und die Funktion im Haus besser bekannt werden. Der Aufwand für die Durchführung und didaktische Aufbereitung liegt hier bei der/dem IT-Sicherheitsbeauftragten.

Klassische Schulungsveranstaltungen sind ein hervorragender Kanal, um das Thema Informationssicherheit zu transportieren und Diskussionen zu unterstützen. Geben Sie den Schulungsteilnehmenden auch im Anschluss Anschauungsmaterial an die Hand, z. B. die wichtigsten, abgeleiteten Regeln bzw. Tipps aus der Veranstaltung, um das gerade erworbene Wissen weiter zu festigen. Auch für den Privatbereich können diese Tipps hilfreich sein und das Thema bei den Beschäftigten aktuell halten. Selbstverständlich sollten zu allen Themen auch im Intranet jederzeit Informationen abrufbar sein.

- **„Backend" der Kampagne:** Das Intranet bietet die ideale Plattform für eine Informations- und Wissenssammlung zum Thema Informationssicherheit, da dort Wissen gesucht, verlinkt und multimedial aufbereitet werden kann. Alle Maßnahmen und Informationen sollten dort hinterlegt werden, dazu gehören auch die Sicherheitsleitlinie, oder die Handlungsempfehlungen, die innerhalb der Kampagne angeboten werden. Die Plattform sollte ab dem ersten Tag der Kampagne bereitstehen, damit interessierte Mitarbeitende direkt an Informationen gelangen.

Sogenannte „E-Learnings" also Lernprogramme können unmittelbar am Arbeitsplatz durchgeführt werden, die Teilnehmenden sind so in der gewohnten Arbeitsumgebung und können sich die Lernzeit selbst einteilen. Gelerntes kann sofort umgesetzt werden.

- **Es müssen aber nicht immer Schulungen sein. Beurteilungskompetenz fördern:** Reines Wissen ist nicht ausreichend, um Gewohnheiten zu unterbrechen. Beschäftigte sollten mit Hilfe regelmäßiger Trainings in ihrer Kompetenz gestärkt werden zu erkennen, wann eine gewohnte Tätigkeit ihre ganze Aufmerksamkeit erfordert, oder wann in einer Stresssituation besonders besonnenes Handeln notwendig ist.

3.2.3 Informationssicherheit langfristig in den Alltag integrieren

Zu diesem Zeitpunkt ist die Belegschaft sensibilisiert und die Informationssicherheit in den Köpfen angekommen. Nun muss dafür gesorgt werden, dass das Thema nicht zu schnell wieder in Vergessenheit gerät und vor allem in den Alltag integriert wird. Der Mensch fällt schnell wieder in seine alten Verhaltensmuster zurück, wenn nicht effektiv und nachhaltig motiviert wurde. Deshalb sollte das Thema immer wieder „aufgewärmt" und damit präsent gehalten werden. Um die Beschäftigten der Behörde wirkungsvoll zu erreichen, können eine Vielzahl unterschiedlicher Kommunikationskanäle genutzt werden. Ein paar Beispiele sind:

Intranet, Newsletter und interne Mails:

Im Intranet können die Kampagne und unterschiedliche Inhalte zur Informationssicherheit publik gemacht werden. Eine dort etablierte Rubrik zur Informationssicherheit bietet sich unter anderem für die Ankündigung von neuen Maßnahmen, Veranstaltungen, Umfragen sowie für die Veröffentlichung von aktuellen Informationen an. Auch anonymisierte Vorkommnisse im Haus können über das Intranet kommuniziert werden. Ein interner Newsletter kann eine Zielgruppe auf den neusten Kenntnisstand halten – beispielsweise mit Hinweisen zur Gefahrenlage, sinnvollen Informationen oder Veranstaltungen.

Gründung von Informationssicherheitszirkeln:

Je häufiger die Beschäftigten über Informationssicherheit sprechen, desto selbstverständlicher werden die notwendigen Verhaltensweisen umgesetzt. Informationssicherheitszirkel sind Zusammenschlüsse (auf freiwilliger Basis) an der Thematik interessierter Beschäftigter, die sich zu Problemen im Umgang mit der Informationssicherheit austauschen. Im Rahmen der Kampagne erhalten die Teilnehmenden aktuelle Informationen zur Thematik und können das IT-Sicherheitsteam im Rahmen von Aktionen unterstützen. Ein Multiplikatoreffekt entsteht, wenn den Teilnehmenden erlaubt wird, z. B. bei Teammeetings in den eigenen Teams regelmäßig kurz über ein IT- Sicherheitsthema zu sprechen.

Informationsmaterial: Die Verteilung von Flyern oder Broschüren in regelmäßigen Abständen greift ein Thema wieder auf. Damit werden auch neue Beschäftigte erreicht, die noch nicht entsprechend sensibilisiert wurden. Auch Plakate oder andere Aufsteller können die Informationssicherheit immer wieder ins Gedächtnis rufen (z. B. Plakat: „Immer dran denken: Passwort sicher bilden").

3.2.4 Umfang und Dauer

Nachdem eine erste Übersicht über die Sensibilisierungsmaßnahmen gewonnen ist, kann über Umfang und Dauer entschieden werden. Die Entscheidung wird dabei nicht nur durch das Budget und die gewünschten Themen beeinflusst. Auch die Struktur und Sicherheits-, Fehler- und Lernkultur des Hauses üben einen Einfluss auf die Entscheidung aus (Beispielfaktoren: „Anzahl der Standorte“, „Welche Maßnahmen passen zur Hauskultur?“, „Welche anderen Kampagnen finden gerade statt?“ oder „Gibt es spezielle Kalenderdaten, die optimal für eine spezifische Maßnahme passen?“)

Eine Kampagne kann aus verschiedenen Modulen bestehen, die sich den einzelnen Themen auch über einen längeren Zeitraum widmen (z.B. sicherer Arbeitsplatz, mobiles Arbeiten, Verhalten in der Öffentlichkeit etc.). Andere Maßnahmen sind eine Informationssicherheitswoche oder sogar der IT-Sicherheitstag, in der die gewünschten Themen „kurz und knackig“ platziert werden.

3.3 Phase III – Durchführung

In den vorherigen Kapiteln wurden alle notwendigen Überlegungen für die Kampagne angestellt und das Sicherheitskonzept erfolgreich aufgebaut: Themen, Zielgruppen und Kanäle sind bekannt und ein Maßnahmenpaket ist vorbereitet, mit dem die drei Bildungsziele „Bewusstsein schaffen“, „Lernen“, „In den Alltag integrieren“ abgedeckt werden. Im nächsten Schritt muss eine Zeitplanung erfolgen, wann welche Maßnahme durchgeführt werden soll. Ein Kampagnenplan mit einer zeitlichen Abfolge kann für die Durchführung eine sehr gute Hilfe sein.

Ein Vorschlag für einen Zeitplan sowie eine Checkliste zur Durchführung von Maßnahmen befindet sich in diesem Leitfaden.

3.3.1 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. Wenn die Entscheidung für eine große oder kleine Kampagne getroffen wurde, sollte zunächst die zeitliche Abfolge der Maßnahmenpakete geplant werden.

Klären Sie, welche anderen Kampagnen für den von Ihnen veranschlagten Zeitraum geplant sind, damit andere Aktionen Ihren Maßnahmen nicht die Aufmerksamkeit streitig machen. Berücksichtigen Sie auch typische Urlaubszeiten oder Zeiten, in denen Ihre Beschäftigten möglicherweise besonders stark eingespannt sind.

- Planen Sie die Maßnahmen mit genügend Abstand voneinander und schließen Sie erst ein Maßnahmenpaket zu einem Thema ab, bevor Sie das nächste starten. Reflektieren Sie jeweils die letzte/n Maßnahme/n und lernen Sie daraus bzw. passen Sie Folgemaßnahmen aus dem Gelernten kontinuierlich an – die Pakete sollten nicht „in Stein gemeißelt sein“.
- Verschieben Sie ggf. auch Maßnahmen, wenn dies notwendig wird, z. B. weil es einen aktuellen Vorfall gab, der zu einer bestimmten Maßnahme gut passen würde, so ziehen Sie diese vor.

- Beziehen Sie besondere Termine in Ihre Überlegungen ein z. B. Urlaubszeit im Juli – Sie könnten einen Flyer mit dem Thema „mobile Sicherheit im Urlaub“ im Juni verteilen. Oder Sie nehmen die Weihnachtszeit zum Anlass für das Thema „sicheres Online-Shopping“. Schauen Sie, wie die festen Termine zu Ihren Themen passen und wie Sie diese transportieren können.

3.3.2 Maßnahmengestaltung

Die Maßnahmen wurden in einem Zeitplan festgehalten und der Ablauf wurde festgelegt. Nun folgt die Überprüfung der Inhalte gemäß der Zielstellung. Die Checkliste aus dem Werkzeugkasten kann dabei wertvolle Hinweise geben. Für jeden Kampagnenbaustein sollten „die fünf W-Fragen“ beantwortet werden:

- Was: Was soll in diesem Modul gemacht werden (z. B. ein Plakat produzieren, eine Trick- Mail versenden, eine Schulung organisieren)?
- Wer: Für wen bzw. für welche der Zielgruppen ist diese Maßnahme relevant – an wen richtet sie sich?
- Wie: Wie soll die Maßnahme umgesetzt werden (z. B. ein Plakat entwerfen, grafische Elemente einbauen, Corporate Design umsetzen, Druckerei beauftragen, Aufhängung der Plakate klären)?
- Wo soll die Maßnahme stattfinden (wo sollen die Plakate aufgehängt werden, wo kann eine Schulung stattfinden)?
- Welche Ressourcen: Welche Ressourcen sind für die Umsetzung notwendig, wen müssen Sie beauftragen (lassen), wer ist mit an der Umsetzung beteiligt (welche Abteilungen)?

Wichtig: Alle Maßnahmen sollten mit den beteiligten Abteilungen im Hause geklärt und die Behördenleitung, soweit erforderlich, in Kenntnis gesetzt werden. Beispiel:

- Wo dürfen Plakate aufgehängt werden (Brandschutz beachten – der Brandschutzbeauftragte hilft sicher gern)?
- Wo verlaufen Fluchtwege, in denen nichts aufgestellt werden darf?

3.3.3 Feinjustierung

Die durchgeführten Maßnahmen sollten fortlaufend überprüft werden. Das Thema Informationssicherheit muss positiv belegt sein, wenn es bei den Beschäftigten verankert werden soll.

Daher sind Nachjustierungen notwendig, um auf die aktuelle Situation bzw. Stimmung im Haus Rücksicht zu nehmen. Fragen Sie, wie jede Maßnahme angekommen ist. Verteilen Sie ggf. Fragebögen an ausgewählte Personen und bitten Sie um Feedback. Jede Maßnahme sollte immer wieder auf diese Punkte überprüft werden:

- Was haben wir zu den Themen erreicht? Sind einzelne Module besonders gut angekommen und lassen sich diese wiederholt einsetzen?
- Gab es Maßnahmen, die zu Verstimmung, größerer Unsicherheit oder Ärger geführt haben?
- Gibt es zurzeit besondere Ereignisse, die für die Beschäftigten vorrangig sind (Umstrukturierungen, Schließung von Standorten, Wahlen, Pandemien)?

- Gibt es Rückmeldung und Erfahrungswerte von Maßnahmen-Beteiligten, die eine Änderung notwendig machen (z. B. Aufsteller in Fluchtwegen, Probleme mit der Anbringung von Plakaten, Umstände für Reinigungspersonal durch Aufkleber etc.)?
- Gibt es Rückmeldung zum Erfolg der Kampagnenbausteine (z. B. vom Helpdesk über Anzahl oder Qualität der Hotline-Anrufe)?

Bleiben Sie mit Ihren Maßnahmen immer flexibel und scheuen Sie sich nicht, einzelne Bausteine zu verschieben oder zurückzustellen, wenn es die Situation erfordert. 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.

3.4 Phase IV – Evaluation

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. In Kapitel 3.1.1 wurden die Ziele der Kampagne festgelegt, die nun evaluiert werden müssen. Auch die Ausgangssituation und die Informationen von beteiligten Kolleginnen und Kollegen (z. B. Helpdesk) vom Beginn der Kampagne geben nun Aufschluss über die Wirksamkeit Ihrer Maßnahmen, z. B.:

- Auswertung der Zugriffe auf das Intranet: Notieren Sie die Zahlen zu Beginn der Kampagne und beobachten Sie den Verlauf der Zugriffszahlen im Laufe der Maßnahmen.
- Fragebögen: Verteilen Sie Fragebögen an ausgewählte Mitarbeitende oder planen Sie eine Evaluationsaktion, z. B. vor der Kantine und befragen Sie Beschäftigte direkt auf Basis eines vorbereiteten Fragebogens (z. B. im Anhang).
- Gespräche: Führen Sie Gespräche mit Beschäftigten, fragen Sie konkret, was als gut/ was als weniger gut empfunden wurde. Fragen Sie auch nach dem subjektiven Eindruck des IT-Teams und der Behördenleitung.
- IT-Helpdesk: Fragen Sie bei Ihrem IT-Helpdesk nach, inwieweit sich die Anfragen verändert haben: erfolgen mehr Anfragen aufgrund erhöhter Sensibilität (à la „ich habe hier eine E-Mail, die mir komisch vorkommt …“), haben die Anfragen ein anderes Niveau/Thema als vorher, sind weniger „Vorfälle“ zu verzeichnen.
- Bewertungen aus dem IT-Sicherheitstag.
- Ergebnisse erneut durchgeführter Tests wie Social Engineering-Angriffe, Trick-E- Mails, etc.
- Auswertungen, Rückflüsse aus/zum Krimi DenkXsicher (Denk mal sicher)

- Zusätzlich existieren auch schwer zu messende „weiche Faktoren“. Mögliche „weiche“ Kennzahlen sind beispielsweise:
  - Geringere Inanspruchnahme der IT-Abteilung durch weniger „verseuchte“ Rechner,
  - Mehr Meldungen von „verdächtigen“ Vorfällen, E-Mails etc. bei der Hotline,
  - Mehr Abrufe von Informationsangeboten (bspw. Intranetseite),
  - Ergebnisse der Kontrollen der Arbeitsplätze durch das Sicherheitsteam (bspw. Zahl gesperrter APCs),
  - Ergebnisse wiederholter Wissensabfragen und Schulungen. Oder wie viele Beschäftigte haben den Bundes-Informations-Sicherheits-Schein – BISS absolviert.

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

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

Üben, üben, üben!

Sie planen eine Informationssicherheitskampagne. Im Team legen Sie bereits folgende Merkmale fest:

1. Die Kampagne soll drei Wochen lang sein.
2. Jede Woche soll eine Botschaft die Zielgruppe erreichen.
3. Berufliche Alltagsgegenstände (Informationsträger) sollen mit Bild und Text bedruckt werden.

Wie gehen Sie vor? Beantworten Sie kurz folgende Leitfragen:

Aufgabe 3 Die Lerninhalte betreffend:

a. Zu welchem Anlass soll die Kampagne starten?
b. Welche Bildungsziele verfolge ich mit den Botschaften?
c. Wie lassen sich die einzelnen Botschaften zu einem Thema zusammenfassen?
d. Welche Stilmittel und Gestaltungselemente unterstützen bei der Erfassung der Botschaft?

Aufgabe 4 Die Zielgruppe betreffend:

a. In welchen Zeiträumen und an welchen Orten erreiche ich meine Zielgruppe?
b. Welche Informationsträger/Alltagsgegenstände eignen sich für die Multiplikation meiner Botschaften, begründen Sie!
c. Wie viele Informationsträger müssen produziert und bereitgestellt werden, damit die vorgesehene Anzahl an informierten Personen erreicht wird?

Aufgabe 5 Den Informationsträger betreffend:

a. Passen die gewählten Stilmittel und Gestaltungselemente in das soziale/kulturelle Bedingungsumfeld der Zielgruppen (Deutung & Interpretation)?
b. Welche Stilmittel und Gestaltungselemente fungieren als Wiedererkennungswert der Kampagne (Analogien)?

Beispiellösung mit Siggi Sicher (Siehe Werkzeugkasten Kapitel 5.1.1)

Zu Aufgabe 3)

Die Kampagne soll als Reaktion zu den neuesten Angriffen auf E-Mail-Konten im Ministerium gestartet werden. Das Bildungsziel ist der handlungssichere Umgang mit Phishing Mails. Dazu sollen Beispielmails gezeigt werden und aktuelle Fälle aufgearbeitet werden, im Episodenstil.

Abbildung 2 BAköV Siggi Sicher

Zu Aufgabe 4)

Die Zielgruppe soll über eine tägliche Haus-E-Mail erreicht werden, damit werden alle Mitarbeitende erreicht.

Zu Aufgabe 5)

In der täglichen Haus-E-Mail (insgesamt 15 E-Mails) werden Kurzgeschichten erzählt mit Beispielen und Fällen. Es gibt immer einen Fall und eine Fallbewältigungsstrategie. Der Aufbau, das Layout und der Stil sind immer gleich. Eine laufende Nummer der Episode und ein spannender Titel sind die Wiedererkennungsmerkmale der Kampagne. Es werden Links eingebaut, die zu weiteren Medien führen.

4. Weiterführende Informationen

Stöbern Sie in verschiedenen Quellen für weiterführende Informationen zum Thema Sensibilisierung, z. B.

- BSI: IT-Grundschutzkompendium ORP.3 Schulung und Sensibilisierung des Bundesamtes für Sicherheit in der Informationstechnik (https://www.bsi.bund.de)
- BAköV-Fortbildungsportal – Werkzeugkasten für die Bundesverwaltung – hier finden Sie eine Fülle an Vorlagen, Texten und Ideen für Ihre Kampagne. (https://lernplattform.intranet.bund.de)
- Allianz für Cybersicherheit (https://www.allianz-fuer-cybersicherheit.de)
- BSI für Bürger (https://www.bsi-fuer-buerger.de)

5. Der Werkzeugkasten

Vorwort

Im Folgenden stellen wir Ihnen beispielhaft Instrumente und Werkzeuge vor, die es Ihnen ermöglichen, die verschiedenen notwendigen Maßnahmen zur Kommunikation der Themen Informationssicherheit und Datenschutz umzusetzen.

Neben einer Vielzahl an Materialien der Bundesakademie für öffentliche Verwaltung (BAköV) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) finden Sie hier Checklisten sowie zahlreiche Tipps und Hinweise, wie Sie die Materialien erfolgreich einsetzen können. Sie werden feststellen, dass nicht alle Materialien für Ihre Behörde geeignet sind — dafür sind die Ausgangspositionen der einzelnen IT- Sicherheitsbeauftragten in den jeweiligen Behörden zu individuell und unterschiedlich.

Dennoch sollten Ihnen die vorliegenden Hilfsmittel eine Orientierung und einige Anregungen für eigene Ideen zur Umsetzung geben und zahlreiche Anknüpfungspunkte für die Umsetzung der Kampagne in Ihrem Haus herstellen.

Verstehen Sie den Werkzeugkasten als Ihr Nachschlagewerk für die Kommunikationsinstrumente, die Sie bei der Durchführung der Kampagne in Ihrem Haus nutzen möchten.

Schauen Sie in den Werkzeugkasten auf dem Fortbildungsportal, dort finden Sie weitere Konzepte und Materialien, die im Behördenumfeld bisher entstanden sind und genutzt werden dürfen oder Ihnen Anregungen geben.

Kontakt BAköV Lehrgruppe 5:
lg5@bakoev.bund.de

5.1 Plakate, Flyer & Co

5.1.1 Wir dürfen vorstellen: Siggi Sicher und Siggilinde

Abbildung 3 BAköV Siggi und Siggilinde Sicher

Siggi Sicher ist die langjährige Identifikationsfigur der Initiative „Sicher gewinnt!“ und gibt ihr damit ein Gesicht. Er steht für die Aspekte Kompetenz im Umgang mit Informationen, Schnelligkeit und Stabilität und ist die geeignete Visualisierung des zu kommunizierenden Anliegens. Daher haben wir Siggi Sicher in die Gestaltung der verschiedenen Kommunikationsmedien integriert.

Jede Behörde kann individuell entscheiden, ob die Verwendung von Siggi Sicher oder einer anderen Figur/Logo in die Kommunikationskultur des eigenen Hauses passt. Wenn Sie sich dafür entscheiden, stehen Ihnen verschiedene Kommunikationsmedien zur Verfügung.

So steht Ihnen Siggi Sicher zur Verfügung:

Kunststofffigur

Die BAköV stellt die kleine Figur aus weichem Kunststoff dem/der jeweiligen IT-Sicherheitsbeauftragten zur Verteilung zur Verfügung.

Aufsteller

Der Aufsteller dient als ein Element der internen Kommunikation, dass die anderen Kommunikationsaktivitäten und Marketingmaßnahmen ergänzt.

Sie können den Aufsteller an prominenten Orten Ihrer Behörde platzieren (Haupteingang, Kantineneingang oder Ähnliches) oder an die Tür des Raumes, in dem eine Veranstaltung zum Thema stattfindet.

Plakate

Die Plakate kommunizieren das inhaltliche Anliegen der Sensibilisierungsinitiative und informieren über Gefahren im Umgang mit Informationen. Siggi Sicher wird in diesen Plakaten als wiederkehrendes Merkmal verwendet. Durch die wiederkehrende Verwendung der Figur Siggi Sicher als das Gesicht der Initiative wird dieses Maskottchen zielgerichtet eingesetzt und die Wirkung der Figur weiter etabliert.

Die Plakate stehen auch ohne Siggi Sicher zur Verfügung (siehe Kapitel 5.1.3).

Flyer

Zur vertiefenden Information wurde ein Flyer erstellt, der sich dem Thema „Informationssicherheit und Datenschutz am Arbeitsplatz“ widmet. Diesen Flyer gibt es mit und ohne Siggi Sicher.

Aufkleber-Motiv

Die Plakatreihe wird ergänzt um Aufkleber, über deren Verwendung ebenfalls der/die IT-Sicherheitsbeauftragte entscheidet.

Bildschirmschoner

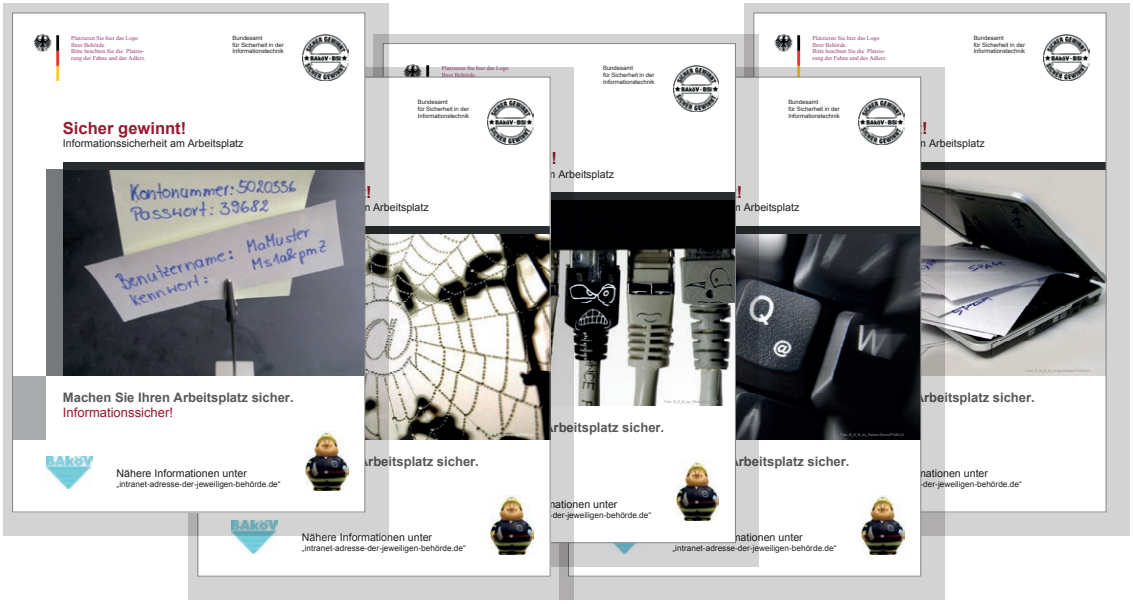
Der Einsatz des Bildschirmschoners als Medium der internen Öffentlichkeitsarbeit bietet ebenfalls die Möglichkeit, Siggi Sicher als „Gesicht“ der Initiative zu etablieren.

Im Fortbildungsportal sind alle Medien des Werkzeugkastens bei der BAköV erhältlich.

Abbildungen 4 BAköV Siggi Sicher

Sicher gewinnt!

Wer ist Siggi Sicher –
Das Vorstellungsplakat



Sicher gewinnt!

Die Kampagnenplakate mit Siggi Sicher-Motiv

5.1.2 Die Werbemedien mit Siggi Sicher

So können Sie die Medien verwenden:

Kunststofffigur

Von der Kunststofffigur können Ihnen nur begrenzte Stückzahlen zur Verfügung gestellt werden. Daher sollten Sie die Verteilung gezielt dort vornehmen, wo Sie das Thema vertiefen wollen:

- an die Teilnehmenden einer Informationsveranstaltung zum Thema,
- im Rahmen einer internen Veranstaltung zum Thema,
- an Kolleginnen und Kollegen, die sich für das Thema interessieren.

TIPP: Fragen Sie vorher bei der BAköV nach, wie viele Figuren Sie abrufen können.

Aufsteller

Der Aufsteller (Leichtmetall) ist ca. 1,00 Meter hoch und kann ideal in Eingangsbereichen platziert werden. Es wirkt am effektivsten, wenn Sie die Figur um Plakatierung und das Auslegen von Info-Flyern ergänzen.

Plakate

Mit der Vorstellung der Figur „Siggi Sicher“ besteht die Plakatserie aus insgesamt sechs Motiven. Wenn Sie sich dafür entscheiden, Siggi Sicher zu verwenden, sollten Sie das Startplakat nutzen, um die Figur „Siggi Sicher“ vorzustellen, um den Start der Kampagne anzukündigen um einen Schulungs-/Seminartermin anzukündigen und um Ihre Kolleginnen und Kollegen in das Thema einzuführen.

Die Plakate stehen Ihnen im Online-Werkzeugkasten der BAköV zur Verfügung. So können Sie Ihr eigenes Behördenlogo einfügen sowie den Hinweis, wo Ihre Kolleginnen und Kollegen weitere Informationen finden. Die Bilder sowie die Platzierung der anderen Logos und Beschriftungen dürfen NICHT verändert werden.

Flyer „Sicher gewinnt!“

Auch die Flyer stehen Ihnen im Online-Werkzeugkasten der BAköV zur Verfügung. Beim Flyer „Sicher gewinnt!“ können Sie Ihr eigenes Behördenlogo an der gekennzeichneten Position (oben links) einfügen. Wenn Sie Textänderungen wünschen, empfehlen wir, sich mit der BAköV wegen des korrekten Corporate Wording in Verbindung zu setzen.

Für den Druck der Plakate und Flyer sprechen Sie bitte Ihre Kolleginnen und Kollegen aus dem Bereich Öffentlichkeitsarbeit an. Sie helfen Ihnen sicher gern weiter.

Bildschirmschoner

Im Fortbildungsportal können Sie sich die Datei mit Siggi Sicher herunterladen und als Bildschirmschoner in Ihrem Haus verwenden.

5.1.3 Die Plakate

Weitere Werbemedien

Wenn Sie sich entschlossen haben, auf den Einsatz von Siggi Sicher zu verzichten, stehen Ihnen noch weitere Plakatmotive zur Verfügung.

Alle Motive visualisieren Themen rund um die Kampagne „Sicher gewinnt!“. Ob „Passwortsicherheit“, „Sicher Surfen im Netz“ oder „sicher E-Mails bekommen und versenden“ – Sie können sich aussuchen, welches Plakatmotiv Ihre Kommunikationsmaßnahmen am effektivsten unterstützt.

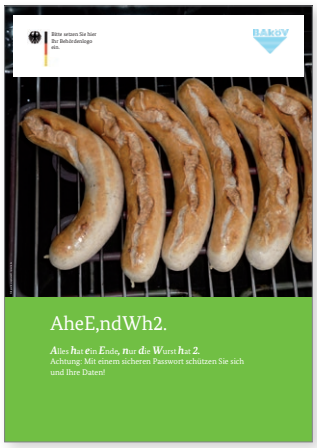
Durch die großflächige Präsenz und eine gezielte Verbreitung im Haus vertiefen die Plakate das Thema „Informationssicherheit“ innerhalb Ihrer Behörde dort, wo Informationstexte nicht mehr greifen.

Die Plakate bieten Ihnen die Möglichkeit, den Beginn der Kampagne zu veröffentlichen, Veranstaltungen, die im Rahmen der Initiative stattfinden, anzukündigen oder das Thema grundsätzlich in Ihr Haus zu bringen. Aufgrund der provokanten Bildsprache ist gewährleistet, dass Ihre Kolleginnen und Kollegen die Plakate bemerken und darüber reden – und sich damit dem Thema „Informationssicherheit“ widmen.

Diese Plakate stehen Ihnen zur Verfügung:

Ihnen stehen neun Plakatmotive zur Verfügung. Sie finden sie in der Online-Version des Werkzeugkastens auf dem Fortbildungsportal.

Die Plakate werden Ihnen als PDF-Dokumente zur Verfügung gestellt. Sie haben damit die Möglichkeit, Ihr Behördenlogo einzusetzen sowie den Hinweis, wo Ihre Kolleginnen und Kollegen weitere Informationen zum Thema bekommen können. Alles Weitere (Logo der BAköV, Überschriften, Farben, Schriften usw.) müssen Sie unverändert übernehmen, ansonsten bitte Rücksprache mit der BAköV. Damit ist ein einheitliches Erscheinungsbild der Kampagne gesichert.



Abbildungen 5 PIXELIO: FotoHiero, RainerSturm, schubalu, siepmannH, Manf-red Walker, René Schellhammer

Sie können die Plakate an prominenten Standorten im Haus platzieren (am Eingang, neben der Zeiterfassung, neben dem Kantineneingang usw.). So ist gewährleistet, dass alle Beschäftigten Ihres Hauses die Plakate sehen und das Thema präsent bleibt.

Alternativ können Sie die Plakate auch als PDF versenden.
Achten Sie dabei bitte auf Barrierefreiheit.

5.1.4 Die Flyer

Die Plakate machen neugierig, die Informationsflyer klären auf. Idealerweise ergänzen Sie Ihre Plakatierung um das Auslegen der Info-Flyer zum Thema „Sicher gewinnt!“ an prominenten Orten wie dem Eingangsbereich, in Sitzungsräumen oder in der Kantine.

Im Zusammenspiel von Plakaten und Flyern erreichen Sie bei Ihren Kolleginnen und Kollegen einen hohen Grad an Aufmerksamkeit, den Sie optional mit der Veröffentlichung von Informationstexten in Ihren internen Medien erweitern können (siehe Kapitel 5.6).

Das Ziel: Das Thema „Informationssicherheit und Datenschutz am Arbeitsplatz“ in die Wahrnehmung Ihrer Kolleginnen und Kollegen bringen, damit sie sich damit beschäftigen und eigenes, beabsichtigtes oder unbeabsichtigtes, Fehlverhalten erkennen und abstellen können.

Diese Flyer stehen Ihnen zur Verfügung

Zur Information über die Initiative „Sicher gewinnt!“ haben wir für Sie zwei Flyer-Varianten erstellt: mit und ohne Ankündigung einer Informationsveranstaltung oder Schulung.

Abbildungen 6 PIXELIO: FotoHiero, RainerSturm, schubalu, siepmannH, Manfred Walker, René Schell-hammer

Ohne Veranstaltungshinweis

Im Innenteil des Flyers machen wir die Lesenden mit dem Thema vertraut. Trojaner, Würmer und Hacking sind für IT-Fachleute bekannte Themen – für Laien nicht. Daher führt der erste Teil langsam ins Thema, während sich der zweite Teil mit sechs „Goldenen Regeln“ verschiedenen Themen der IT-Sicherheit widmet.

Auf der Rückseite finden die Lesenden Hinweise, unter welchen Internetadressen weitere Informationen zum Thema zu finden sind. Außerdem aufgeführt: Das Impressum, in dem Sie bitte die Ansprechperson Ihrer Behörde benennen (den/ die IT-Sicherheitsbeauftragte oder IT-Leitung).

Mit Veranstaltungshinweis

Der Innenteil ist identisch.

Die Rückseite bietet die Möglichkeit, geplante Seminare, Schulungen oder Events anzukündigen, die Referenten vorzustellen und Hinweise zu Zeit und Ort zu geben. Beim Impressum gilt dasselbe wie beim vorigen Flyer.

So können Sie die Flyer verwenden

Die Flyer Vorlagen werden Ihnen als PDF-Dokument zur Verfügung gestellt. So haben Sie die Möglichkeit, die Inhalte des Flyers Ihrem individuellen Bedarf anzupassen. Bei größeren inhaltlichen Veränderungen empfehlen wir jedoch die Abstimmung mit der BAköV.

Bitte platzieren Sie auf der Titelseite Ihr Behördenlogo an der entsprechenden Stelle und ergänzen Sie die Inhalte, wenn Sie Hinweise auf Veranstaltungen o. ä. geben wollen. Vergessen Sie nicht die Kontaktangabe unter „Impressum“.

Beim Druck der Flyer sind Ihnen Ihre Kolleginnen und Kollegen aus der Öffentlichkeitsarbeit sicher gern behilflich. Alternativ können Sie die Flyer auch als PDF versenden. Achten Sie dabei bitte auf Barrierefreiheit.

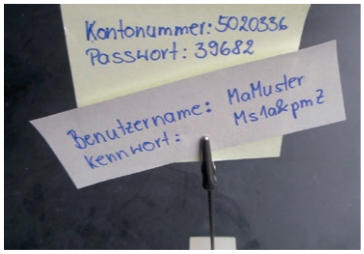
Die Flyer-Vorlagen finden Sie in der Online-Version des Werkzeugkastens auf dem Fortbildungsportal.

5.1.5 Die Bilder

Mit hohem Wiedererkennungswert:

Zur Visualisierung des Themas „Informationssicherheit und Datenschutz am Arbeitsplatz“ wurden Fotomotive ausgewählt, die sich den einzelnen Aspekten dieses Themas widmen:

So gibt es sowohl für das Thema „Passwortsicherheit“ als auch „Sicher mailen“ oder „Sicher im Netz“ eine entsprechende Bebilderung. Die Fotos stehen allen Bundesbehörden zur Verfügung, um in den eigenen Hausmedien verwendet zu werden.

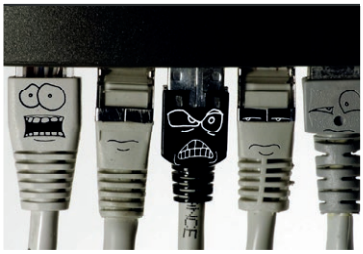


Wie sicher ist Ihr Passwort?

Abbildung 7 Deutsches Patent- und Markenamt

Was tun, bei SPAM-Flut?

Abbildung 8 PIXELIO:_K_B_by_Antje_Delater



Keine Angst vor Hardware

Abbildung 9 PIXELIO:R_K_B_by_Klicker

Abbildung 10 PIXELIO:Mobil arbeiten: R_K_B_By_Rainer-Sturm

Sicher im Netz!

Abbildung 11 Pixelio: R-by_pepsprog

Achtung Datenklau!

Abbildung 12 PIXELIO/Datenklau: R_K_B_by_Antje_Delater

Sicher@Bund.de

Abbildung 13 Pixelio: R_K_B_By_Rainer-Sturm

Wenn Sie die Fotos darüber hinaus selbst zur Kommunikation verwenden möchten, achten Sie bitte auf die Berücksichtigung der Bildrechte.

So stehen Ihnen die Bilder zur Verfügung

Die Fotos

Alle Fotos werden Ihnen als Druckversion mit 300 dpi in einem jpg-Format zur Verfügung gestellt. So können Sie die Bilder zum Druck, aber auch für Online-Anwendungen verwenden.

Da es sich bei den Fotos um lizenzfreie Bilder handelt, werden keine Lizenzgebühren fällig, wenn Sie sie nutzen möchten. Sie sind lediglich verpflichtet, mit der Angabe des Fotografen oder der Fotografin dem Copyright nachzukommen.

Bitte verwenden Sie folgende Copyrightangaben:

Spamflut: R_K_B_by_Antje_Delater/PIXELIO
Passwort: Deutsches Patent- und Markenamt (DPMA)
Mobil arbeiten: R_K_B_By_Rainer-Sturm/PIXELIO
Hardware: R_K_B_by_Klicker/PIXELIO
Datenklau: R_K_B_by_Antje_Delater/PIXELIO
Sicher im Netz: R_by_pepsprog/PIXELIO
sicher mailen: R_K_B_By_Rainer-Sturm/PIXELIO

Sie finden die Bilder auf dem Fortbildungsportal https://lernplattform.intranet.bund.de in der Online-Version des Werkzeugkastens.

So können Sie die Bilder verwenden

Sie finden im Kapitel 5.1 Flyer und Plakate, die bereits mit den Bildern arbeiten. Darüber hinaus können Sie die Fotos zur Bebilderung des Themas in Ihrem hausinternen Intranet, in internen Textpublikationen, Newslettern o.Ä. verwenden.

Die vorliegenden Motive wurden zur Visualisierung der Kampagne ausgesucht. Bitte arbeiten Sie ausschließlich mit diesen Motiven. Wenn Sie ein anderes Motiv haben möchten, wenden Sie sich an die BAköV.

5.2 Die Moderationskarten

Abbildung 14 BAköV: Moderationskarten

Risiken oder Probleme im Kontext von Informationssicherheit sind nicht nur auf die verschiedenen technischen oder organisatorischen Bedingungen zurückzuführen. Sie sind eine Folge unterschiedlicher Ausprägungen der jeweiligen Behörden-, Sicherheits-, Fehler- und Lernkultur. Auch in Behörden mit sich überschneidenden Aufgaben bilden sich an verschiedenen Standorten sehr unterschiedliche Umgangsformen, die unterschiedliche Herangehensweisen in der Kommunikation – insbesondere von Sicherheitsthemen – erfordern.

Gerade die Unterschiede in der Bewertung von menschlichem „Fehlverhalten“ und weiteren Risiken erfordern bereits in der Planungsphase von nachhaltigen Kommunikationsmaßnahmen eine Differenzierung der einzelnen Maßnahmenbausteine. Ziel ist es, durch die Analyse der Problemstellungen die geeigneten Maßnahmen zu ermitteln und zielgruppengerecht umzusetzen.

In diesem Zusammenhang ist es wichtig zu erkunden, welche Zielgruppe mit welchen

Aufgaben und Verantwortlichkeiten mit welchen Botschaften angesprochen werden sollen.

Wo gibt es in Ihrem Haus die größten Lücken in Bezug auf „Informationssicherheit“? Wie offen wird mit Fehlern und Problemen umgegangen? Welche Zielgruppe hat den größten Sensibilisierungsbedarf? Und welche Zielgruppe können Sie als Mitstreitende und Multiplikatoren gewinnen?

„Sicher gewinnt! – die Moderationskarten“ sind ein Workshop-Instrument, mit dessen Hilfe Sie die Sensibilisierungsinitiative zum Thema Informationssicherheit effizient vorbereiten, planen und durchführen können. Die Moderationskarten, die als Instrument auf „Teil I – Der Sensibilisierungsleitfaden“ aufbauen, tragen der Kulturvielfalt der Behörden Rechnung. Sie versuchen, die Beteiligten in den Sicherheitsbereichen

„zum Sprechen“ zu bringen und unterschiedliche Kommunikationsniveaus auszugleichen. Dabei wird die Vielfalt von Kommunikation auf das Wesentliche verdichtet und in „geordnete Bahnen“ navigiert.

Das Moderationskartenset besteht aus insgesamt 112 Karten in den vier Kategorien:

- BILDER
- THEMEN (darunter eine Blanko-Karte)
- ZIELGRUPPEN (darunter eine Blanko-Karte)
- KANÄLE (darunter eine Blanko-Karte)

Die Inhalte sind auf Basis praktischer Erfahrungen und methodischen Vorgehens über einen Zeitraum von fünf Jahren erarbeitet worden. Mit dem Fokus auf Beschäftigtensensibilisierung haben Expertinnen und Experten aus dem Bereich Kommunikation und Psychologie die Karten auf die Sensibilisierungskampagne „Sicher gewinnt!“ angepasst.

Sie können bei Bedarf mit Hilfe von „Jokern“ in Form von Blanko-Karten und einer zusätzlichen Dokumentenvorlage eine individuelle Erweiterung vornehmen – und die Karten so Ihrem Bedarf anpassen.

Bei Interesse fragen Sie in der LG 5 nach.

Die Moderationskarten:
Lernkarten als Abbild des Sensibilisierungskonzeptes

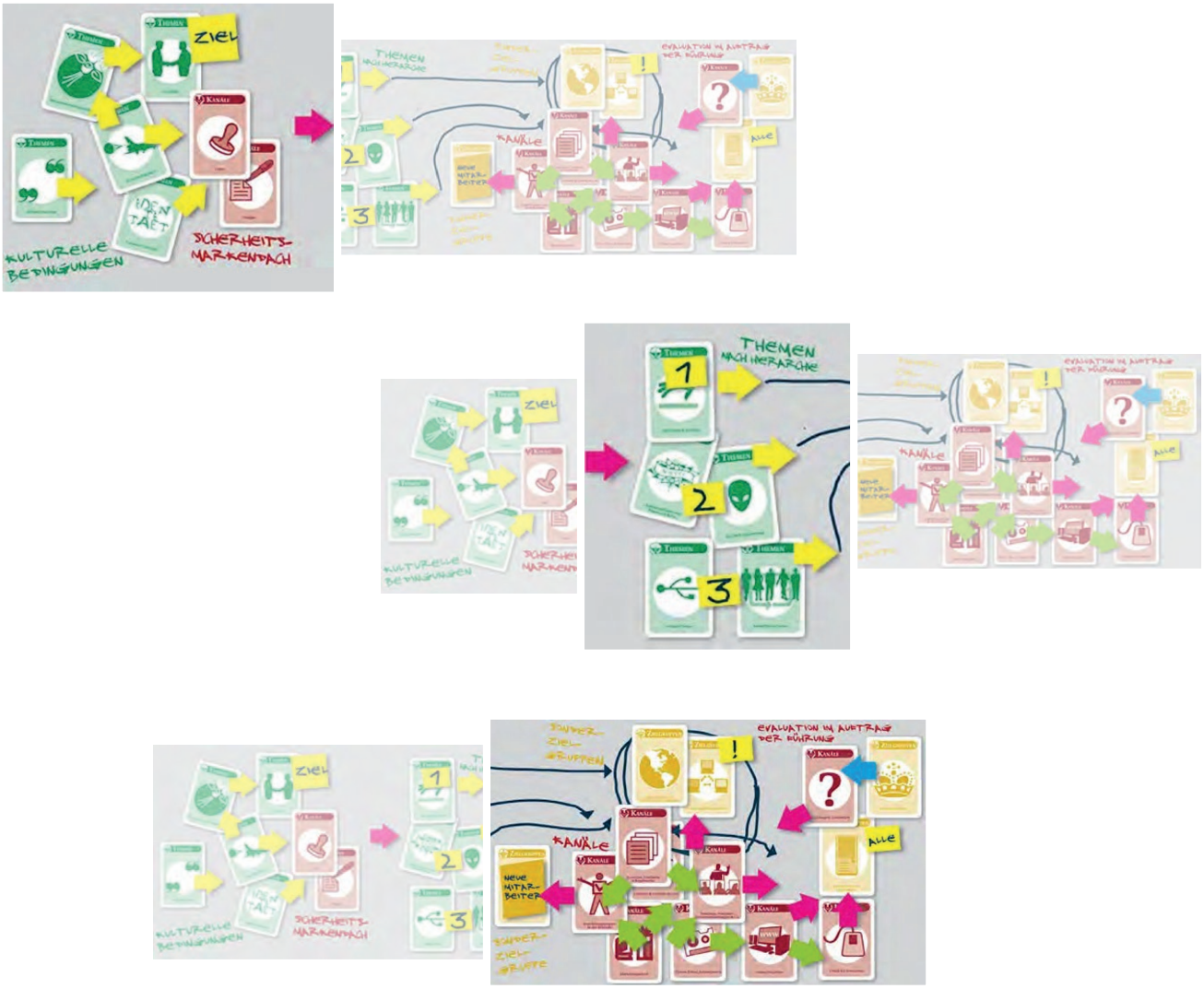


Abbildung 15 BAköV: Moderationskarten

So arbeiten Sie mit den Moderationskarten

Beginnen Sie die Arbeit mit den Karten in einer frühen Phase der Kampagnenplanung. Sie werden erstaunt sein, wenn die Karten zu „sprechen“ beginnen und vieles von dem ausdrücken, was eigentlich gemeint ist, oft aber nicht (offen) gesagt werden kann.

Es ist der Vielfalt der Informationssicherheit geschuldet, dass keine Sensibilisierungsinitiative sämtliche Aspekte des Themas über Trainings und andere Kommunikationsmaßnahmen abdecken kann. Unterschiede zeigen sich nicht nur aufgrund der heterogenen Strukturen an unterschiedlichen Standorten mit den verschiedenen Aufgaben, sondern auch in der Wahrnehmung von „Schmerzpunkten“ durch IT-Sicherheitsbeauftragte.

Verschiedene Risiken – zahlreiche Themen

Obwohl jede Behörde ähnlichen Risiken ausgesetzt ist, können Bewertungen und Top-Listen von Risiken oder tatsächlichen Vorfällen sehr unterschiedlich ausfallen. Und mehr noch: Risiken betreffen möglicherweise nicht sämtliche Beschäftigtengruppen im gleichen Umfang:

- Die einen IT-Sicherheitsbeauftragten „leiden“ daran, dass Kolleginnen und Kollegen häufig Ihre Passwörter vergessen,
- für andere spielt das Thema „Social Engineering“ eine größere Rolle.

Die THEMEN-Karten dokumentieren Inhalte für Sensibilisierungsmaßnahmen, die der Sachlage entsprechend ausgewählt werden.

Vielfältige Aufgaben – unterschiedliche Zielgruppen

Tägliche Arbeit am PC, mobiles Arbeiten, stationärer Arbeitsplatz, IT-Profis, IT-Laie, Führungskraft – wir haben die Besonderheiten von Beschäftigten in puncto Bildung, Aufgaben, Rollen und Risiken sowie ihre unterschiedlichen Bezugspunkte zur Informationssicherheit und die potenzielle Wirkung von Sensibilisierungsmethoden und -medien differenziert. Dafür haben wir neben den Karten der Kategorie THEMEN auch ZIELGRUPPEN-Karten geschaffen, die ein grobes Raster der Beschäftigtenstruktur im Hinblick auf den Datenschutz und die Informationssicherheit am Arbeitsplatz repräsentieren.

Das Ziel dieser Sensibilisierungskampagne ist es, die verfügbaren Kommunikationsmedien dort gezielt einzusetzen, wo sie potenziell die größtmögliche Wirkung erzielen. Daher ist es Ihre Aufgabe, besonders die Zielgruppen anzusprechen, bei denen Sie das höchste Gefahrenpotenzial vermuten und bei denen der Bedarf an Aufklärung am höchsten ist.

Vielfältige Medienwelt – unendlich viele Kanäle

Über die KANÄLE-Karten versetzen wir uns in die Lage, die Informationswege zu bestimmen, auf denen unsere Botschaft mit den „richtigen“ Themen zu den ausgewählten Zielgruppen gelangt. Doch welche Kanäle unserer internen Kommunikation funktionieren gut? Und welche nicht? Existieren neue, noch nicht erprobte Kanäle, die aufgrund ihres innovativen Charakters Aufmerksamkeit verheißen? Diese und weitere Fragen können Sie mit den Karten der Kategorie KANÄLE beantworten.

5.3 Das Lernspiel „Quer durch die Sicherheit“

Sicher gewinnt! – ganz spielerisch:

Das Lernspiel „Quer durch die Sicherheit“ ist ein lehrreicher wie unterhaltsamer Mix aus Security-Quiz und Zug-um-Zug-Strategiespiel. Basierend auf 49 Quizkarten mit Fragen zum Thema sowie mit überdimensional großen Würfeln und Spielfiguren entstand ein begehbares Riesenspiel, bei dem die Mitspieler und Mitspielerinnen jederzeit auch die Spielfiguren ersetzen können, um Teil des Spiels zu werden.

Als Brettspiel angelegt unterstützt das Lernspiel die Kampagne fantasievoll. Es beinhaltet breit angelegte Fragen rund um das Thema Informationssicherheit und ist für eine Spielgruppengröße ab zwei Spielenden möglich, ab vier Spielenden jedoch besser geeignet. Ziel ist es, durch das korrekte Beantworten der Fragen mit der eigenen Spielfigur das Zielfeld zu erreichen. Dabei kommt ein Würfel zum Einsatz, der das Fortkommen der Spielfiguren bestimmt.

Das Spiel weckt Aufmerksamkeit. Es macht Spaß, vermittelt Lerninhalte und unterstützt die Sensibilisierungskampagne nachhaltig. Die Fragen regen Diskussionen unter den Teilnehmenden an, die Aufteilung in mindestens zwei Spielgruppen sorgt für Konkurrenz und Wettbewerb. Die Fragen des Spiels drehen sich um die Informationssicherheit am Arbeitsplatz, sensibilisieren zu Themen wie Computerviren und -würmern und zeigen Wege auf, wie diese Gefahren zu vermeiden sind. Nutzen Sie diese Aufmerksamkeit, um andere Kommunikationsmaßnahmen im Rahmen der Kampagne zu bewerben.

Abbildung 16 BAköV: Quer durch die Sicherheit

So steht Ihnen das Spiel zur Verfügung

Das Spiel als Groß- oder Kleinformat

Das Lernspiel „Quer durch die Sicherheit“ wurde in zwei Varianten an die Sensibilisierungsinitiative der Bundesverwaltung angepasst. Für das Großformat ist eine Fläche von 5 × 5 Metern und für das Tischspiel 1 × 1 Meter erforderlich.

Aufsteller

Der Effekt des Spiels wird verstärkt, wenn alle sofort verstehen, wie das Spiel funktioniert. Dafür sorgt ein großer Aufsteller, der die Spielregeln auflistet und der gleichzeitig als Eyecatcher für das Publikum dient. Der/ die IT-Sicherheitsbeauftragte übernimmt die Rolle der Spielleitung.

Beide Spielvarianten sowie der Aufsteller können bei der BAköV ausgeliehen werden.

So können Sie das Spiel verwenden

Das Spiel soll Veranstaltungen zum Thema Informationssicherheit begleiten oder auch bei internen Führungskräfterunden eingesetzt werden.

Damit eignet sich das Großformat für einen Einsatz im Rahmen eines Informations-Events, eines „Tag der offenen Tür“, weiteren internen und/oder externen Informationsveranstaltungen wie beispielsweise:

- bei Seminaren
- bei Veranstaltungen von Führungskräften
- im Rahmen eines Roadshow-Hacking
- einem IT-Sicherheitstag oder
- für Veranstaltungen der Behörde (Tag der offenen Tür).

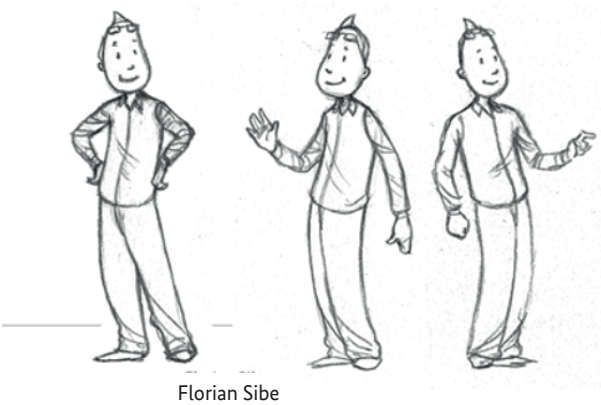
5.4 Sicher gewinnt! – Die Lernwelt

Kennen Sie Lisa, Susanne und Florian Sibe?

In vielen Behörden nehmen Beschäftigte an
der Veranstaltung „Informationssicherheit und Datenschutz am Arbeitsplatz“ teil.

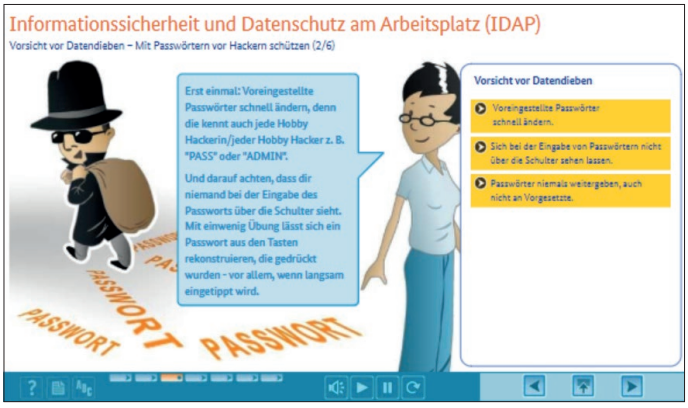
Die Teilnehmenden sollen Maßnahmen zur
Informationssicherheit und zum Datenschutz kennenlernen, die

- sie eigenverantwortlich im Umgang mit Daten und IT am Arbeitsplatz anwenden sollen,
- die sie als vorgegebene zentrale Sicherheitsmaßnahmen einhalten bzw. nutzen sollen.



Florian Sibe

Susanne



Lisa

Abbildungen 17 BAköV: Lernwelt

Die wesentlichen und weiterführenden Inhalte sind in einem Skript zusammengefasst, das nach Abschluss der Veranstaltung ausgehändigt wird.

Für alle diejenigen, die die Inhalte vertiefen möchten oder die keine Gelegenheit zur Teilnahme an einer Veranstaltung hatten, gibt es auch eine Online-Version der Inhalte.

In dieser Online-Version werden die gewünschten Hinweise zum individuellen Abruf zur Verfügung gestellt. Die Inhalte vermitteln den Lernenden Wissen zu den Anforderungen an die Informationssicherheit und den Datenschutz am Arbeitsplatz und ermöglichen den erfolgreichen Abschluss des Onlinetests zum Erwerb des „Bundes-Informations-Sicherheits- Schein“ (BISS, mehr dazu in Kapitel 5.5). In der Online-Version werden u.a. folgende Themen behandelt:

- Informationssicherheit – Warum? (Verfügbarkeit-Vertraulichkeit-Integrität; Schwachstellen, Bedrohungen, Risiken, Schäden)
- Richtiger Einsatz von Passwörtern
- Computersicherheit – Sperren des Rechners / Verhalten bei Schadsoftware
- Umgang mit personenbezogenen Daten
- Umgang mit E-Mail
- Vorbeugung gegen Social Engineering und Informationssicherheit außerhalb des Büros

In der Version 2021 ist die Lernwelt modularisiert worden, somit sind jetzt auch einzelne Themen separat aufzurufen. Die Lernwelt kann folglich weiterhin als Ganzes oder passgenau und mit geringem Zeitaufwand absolviert werden.

Ebenso ist es möglich, die Standardthemen der Lernwelt mit behördenspezifischen Themen zu ergänzen. **Bevor jedoch über den BAköV-Rahmenvertrag eigene Lernprogramme oder Ergänzungen abgerufen werden können, ist stets zu prüfen, ob die Lernwelt wirklich nicht ausreicht.**

Der Ausdruck eines Zertifikates ist auch für einzelne Themen möglich. Die Lernwelt finden sie auf dem Fortbildungsportal der BAköV.

Der Ausdruck eines Zertifikates ist auch für einzelne Themen möglich.

Die Lernwelt ist von jedem Arbeitsplatz in der Bundesverwaltung aus erreichbar, Sie finden sie auf dem Fortbildungsportal der BAköV.

So können Sie die Lernwelt verwenden

Informieren Sie darüber, dass es diese Online-Lernwelt zur Informationssicherheit und zum Datenschutz gibt. Nutzen Sie interne Medien wie Rundschreiben, Schwarzes Brett, Intranet oder Newsletter zur Verbreitung der Inhalte und klären Sie über den Nutzen der Webwelt auf.

Geben Sie sich als Ansprechperson für Rückfragen an – eine gute Gelegenheit, sich im Haus zu positionieren.

Der Bundes-Informations-Sicherheits-Schein

5.5 Holen Sie sich den BISS

Der Bundes-Informations-Sicherheits-Schein steht für Wissen. Denn er bestätigt allen, die ihn bekommen, korrektes Wissen rund um das Thema „Informationssicherheit und Datenschutz am Arbeitsplatz“ und den richtigen Umgang mit Informationen.

Um den BISS zu bekommen, muss lediglich ein entsprechender Test bestanden werden.

Alle sollten sich in der Online-Lernwelt mit den Themen rund um die Informationssicherheit auseinandersetzen. Weiteren Materialien wie beispielsweise das E-Learning zum Datenschutz können zur Vorbereitung für den BISS-Test genutzt werden.

Es ist das Ziel jeder Behörde, eine möglichst hohe Teilnahmequote beim Erwerb des Bundes-Informations-Sicherheits-Scheins zu erreichen. Nach Bestehen des Tests kann sich jede teilnehmende Person ein Zertifikat ausdrucken und der/dem jeweiligen IT-Sicherheitsbeauftragten zur Kenntnis geben. Der/die IT-Sicherheitsbeauftragte kann dann darüber entscheiden, wie und auf welchem Weg das Maß der Beteiligung am BISS-Test innerhalb der eigenen Behörde kommuniziert wird.

Nach dem Ende einer Kampagne kann der Test weiterhin verwendet werden:

- bei der Schulung/Sensibilisierung neuer Bundesbediensteter,
- bei der regelmäßigen Auffrischung der Nutzungsbedingungen von mobilen elektronischen Medien wie Token, Laptop usw.

5.6 Die Informationstexte

Informieren Sie Ihr Haus:

Ergänzen Sie die Plakatierung und die Auslage von Info-Flyern um die Veröffentlichung von Informationstexten in Ihren internen Medien wie beispielsweise Newsletter, Intranet, Schwarzes Brett und/oder Rundschreiben.

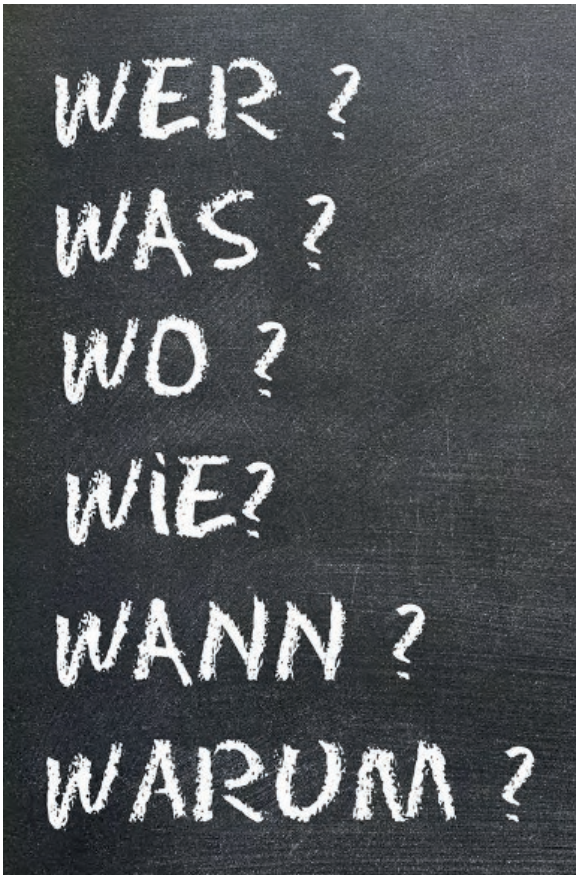


Abbildung 18 Fotolia: Informationstexte

Diese Texte stehen Ihnen zur Verfügung

Der Informationstext vor dem Start der Kampagne

Wir haben Ihnen Mustertexte in drei verschiedenen Längen zusammengestellt, die Sie vor Beginn der Kampagne als Information vorab veröffentlichen können.

Sie informieren alle Beschäftigten über das Warum (warum widmet sich unser Haus diesem Thema?), über das Was (was für eine Kampagne startet hier?), das Wie (wie wird die Kampagne umgesetzt?) und das Wann (wann starten die Veranstaltungen?).

Die Informationstexte zum Start der Kampagne

Wenn die Schulungstermine feststehen, setzt sich die Kommunikationskette fort.
Hierfür haben wir für Sie drei verschiedenen Textvarianten zusammengestellt:

- Text für Mitarbeitende
- Text für Führungskräfte
- Text für IT-Fachleute

Sie können, je nach Zielgruppe, Ihre Kommunikation gezielt ausrichten und die jeweiligen Kontaktpersonen als Multiplikatoren in Sachen „Informationssicherheit und Datenschutz“ gewinnen.

Die Texte geben Zeit und Ort der Veranstaltung(en) bekannt und gewähren einen kurzen Einblick auf den zu erwartenden Inhalt.

Die Texte für Führungskräfte und IT- Fachkräfte appellieren an die besondere Verantwortung derselben und rufen zur Unterstützung bei der Vermittlung der Inhalte zum Thema „Informationssicherheit und Datenschutz“ auf.

TIPP: Lassen Sie sich die Texte von der Leitung Ihrer Behörde unterschreiben. Das verstärkt den Eindruck, dass die Themen „Informationssicherheit und Datenschutz“ für Ihr Haus von besonderer Bedeutung sind.

Alle Texte finden Sie im Werkzeugkasten.

5.7 Seminare / Events / Theater / Filme

Darf es noch etwas mehr sein:
Informationen sind gut – Veranschaulichung ist besser.

Was überzeugt mehr als die Praxis? Nichts! Deshalb können Sie Ihre kommunikativen Aktivitäten mit der Veranstaltung von Schulungen oder anderen Events effektiv unterstützen.

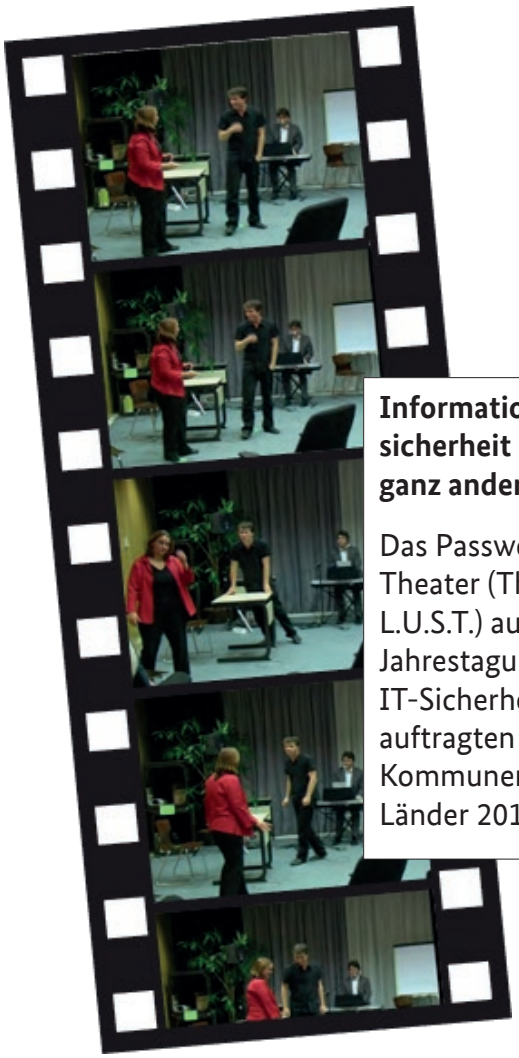
Schulungen

Stimmen Sie sich mit den externen beratenden oder vortragenden Personen ab, wann Sie für wen ein Seminar/Webinar mit welchen Inhalten veranstalten möchten (Ihre Ansprechpersonen können Sie bei der Lerngruppe 5 der BAköV erfragen)

Events

Sehr eindrucksvoll, aber auch sehr eindringlich kann das Thema „Informationssicherheit“ anhand einer Hacker-Demonstration gezeigt werden. Sie werden staunen, wie rasch ein vermeintlich sicheres Passwort geknackt ist und wie schnell Externe Zugriff auf Ihren PC bekommen.

Sprechen Sie die BAköV an. Hier wird Ihnen gern der Kontakt vermittelt.



Informationssicherheit mal ganz anders

Das Passwort-Theater (Theater L.U.S.T.) auf der Jahrestagung der IT-Sicherheitsbeauftragten der Kommunen und Länder 2010

Abbildung 19 BaköV, Foto Jahrestagung 2010

Passwort-Theater – ein Improvisationstheater

Sie wollen das Thema Informationssicherheit einmal auf außergewöhnliche Weise präsentieren? Sie wollen ein bestimmtes Thema theatralisch vermitteln.

Oder wollen Sie das Sommerfest oder eine andere Veranstaltung mit einem interaktiven Element bereichern?

Das Passwort-Theater ist ein Improvisationstheater und hat viele Gesichter: Lassen Sie sich überraschen! Alle Showformate sind geprägt von spontaner Comedy, Wortwitz und Situationskomik, gewürzt mit zahlreichen musikalischen Einlagen.

Alles entsteht improvisiert vor den Augen der Zuschauer, die dabei eine wichtige Rolle spielen. Zum Beispiel sammeln die Darstellenden vor jeder Szene drei Vorschläge für einen Titel oder einen Ort und lässt das Publikum dann durch Klatschen oder Rufen darüber abstimmen, welcher der Vorschläge gespielt werden soll.

Mögliche Auftrittsdauer: 20 bis 120 Minuten.

Sie können sich vorab einen ersten Eindruck verschaffen. Die BAköV hält für Sie eine DVD mit einem 60-minütigen Auftritt dieses Improvisationstheaters bereit.

Filme

Es ist eine Frage des Budgets, aber grundsätzlich können Sie Ihre Kommunikationsaktivitäten um einen Info-Film zum Thema ergänzen. Bitte sprechen Sie hierfür die BAköV direkt an, um erste Ideen und Möglichkeiten der Umsetzung zu eruieren.

5.8 Die bewegten Bilder – Filme

Licht an, Kamera läuft, und ... bitte

Abbildung 20 BAköV: Film Datenkabel

Bewegte Bilder, Filme und Comics können nachhaltig zur Awareness beitragen. Der Einsatz im Intranet, bei Veranstaltungen oder auch auf einem öffentlichen Bildschirm weckt die Aufmerksamkeit und kann weitere Maßnahmen vorbereiten beziehungsweise ankündigen.

Themenfilme

Die Filme visualisieren in kurzen Geschichten das Verhalten rundum Passwort, E-Mail, Social Engineering, mobiles Arbeiten, Internet, Netzwerke und Malware.

Sie sind damit perfekt geeignet, das Thema beispielsweise im Intranet anschaulich darzustellen. So unterstützend diese Filme nachfolgende erklärende Texte zum Thema, die ohne diese Filme vielleicht ein wenig zu technisch geraten könnten.

Filmclips

Haben Sie gesehen, wie sich die „Stecker“ über Risiken am Arbeitsplatz und das damit verbundene Verhalten unterhalten?

Diese kurzen Filme, dem Sensibilisierungsfilm des Bundesministeriums für Verteidigung entnommen, können getrennt eingesetzt werden und zeigen unterhaltsam, worum es geht.

Persönliche Ansprache

Wenn es in die Kommunikationskultur Ihres Hauses passt, können Sie diese kleinen Filme, die auf jede Behörde übertragbar sind, um eine individuelle und persönliche Ansprache einer offiziellen Vertretung Ihres Hauses ergänzen (z.B. Behördenleitung, Staatssekretär(in), IT-Leitung). Das verstärkt die Nachhaltigkeit, mit der Sie die Themen „Informationssicherheit und Datenschutz“ in Ihrem Haus platzieren. Auf dem Fortbildungsportal finden Sie dazu Beispiele.

Sprechen Sie die BAköV an.

5.9 Der BAköV-Krimi Denk × sicher

Die Kampagne ist analog zu einer Kriminalgeschichte gestaltet. Die Dauer der Kampagne beträgt 12 Monate und kann jederzeit im Jahr gestartet werden. Die Informationsträger wie Plakate, Videos und Büro-Alltagsgegenstände können auch unabhängig der „geschlossenen“ Kampagne verwendet werden. Das Bildungsziel ist der sichere Umgang mit Daten, insbesondere der Umgang mit Phishing-E-Mails und das Verfahren im Falle einer Erpressung. Die Informationsträger werden im Wesentlichen als digitale Medien bereitgestellt.

Denk X sicher

Kampagne mit Krimi – Denk × (mal) sicher!

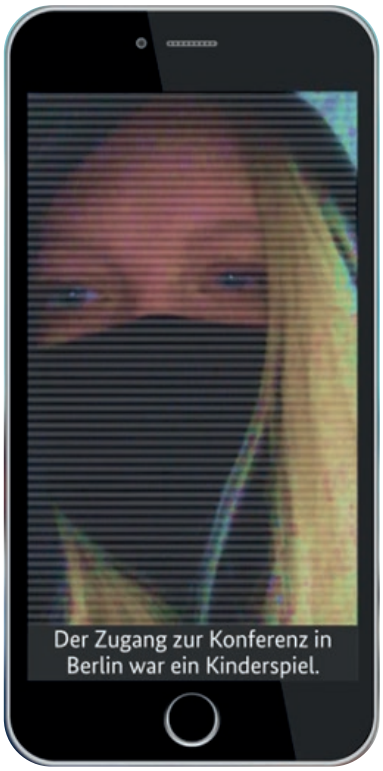
Handlung im Krimi	Monat	Medium (Informationsträger)
Emma, Martin und Stefan arbeiten in einem Ministerium und sind jeden Tag mit der Informationssicherheit konfrontiert. Herr Mangel ist auch ein Kollege, aber nicht sonderlich beliebt. Emma nutzt Partnerbörsen und geht sehr offen mit ihren Daten um. Martin ist auch aktiv, postet Surfer-Bilder und auch seine Freunde posten öffentlich Bilder von ihm. Darunter sind Bilder von ausgelassenen Strandpartys, insbesondere von der letzten Strandparty wurden diffamierende Bilder von ihm veröffentlicht. Herr Mangel bemerkt das. Martin vergisst oft seine Bürotür zu schließen und sperrt auch nicht den Bildschirm.	Monat 1	**Animationsfilm** Vorstellung von Emma, Martin und Stefan im Arbeitsbereich mit (per E-Mail an alle MA) Handlungsfehlern/Botschaften  *Abbildung 21 ML: Krimi – Denk × sicher Film*

Emma, Martin und Stefan (Referatsleiter) besuchen eine Konferenz in Berlin.	Monat 2	**Digitale Postkarte** Haben Sie Ihre Daten noch im Griff?  *Abbildung 22 ML: Krimi – Alles im Griff?*
Emma und Martin werden beide mit einer Phishing-Mail erpresst und sollen 250,– € bezahlen, damit keine privaten Partyfotos veröffentlicht werden.	Monat 3	**Erpresser-E-Mail 1**
Emma ist geschockt, sie hat ganz sicher keine Partyfotos ins Netz gestellt. Daher sucht sie Hilfe bei Stefan.	Monat 4	**Plakat** Phishing-Mail: Stress? 3-Sekunden-Check hilft … Sind Absender, Betreff und Inhalt ok? Wenn nein – melden!  *Abbildung 23 ML: Krimi – Alles im Griff?*

Sie hat danach ein weiteres Problem – sie hat das Passwort ihres E-Mail-Postfachs vergessen, darüber kommt sie mit Stefan ins Gespräch.	Monat 5	**Plakat** Wie lautet Dein Passwort?  *Abbildung 24 ML: Krimi – Passwort?*
Martin bezahlt die 250 Euro, weil er sich peinlich ertappt fühlt, Freunde hatten unangenehme Partybilder mit einem Social Media Account verknüpft. Die Erpressung geht weiter, der Hacker/die Hackerin fordert nun sensible Daten.	Monat 6	**Erpresser-E-Mail 2 an Martin**

Eigentlich sollte Martin nun cool bleiben und endlich den Vorfall melden, stattdessen verzweifelt er und empfindet das ganze Internet als datenklauendes Monster!	Monat 7	**Plakat** Fehler im Internet können schnell an die Haut gehen!  *Abbildung 25 ML: Krimi – Fehler im Internet …* **Block mit Klebezetteln „Cool bleiben“**
Die Informationssicherheit ist ein bedeutsames Thema, die Ministerien sensibilisieren ihre Mitarbeitenden mit Merksätzen.	Monat 8	**Seitenranddruck „Botschaften“ für Schreibblock** 10 Botschaften
Herr Mangel hat gemerkt, dass irgendetwas vorgeht, er beobachtet seine Kolleginnen und Kollegen genau. Martin vergisst oft seine Bürotür zu schließen und sperrt auch nicht den Bildschirm, deswegen weiß Herr Mangel von der Erpressung, er hat in Martins E-Mail-Postfach die Erpressermails gelesen. Nun beschwert er sich bei Martin und fordert ihn auf den Sicherheitsbeauftragten zu informieren. Martin verdächtigt Herrn Mangel, ihn erpresst zu haben!	Monat 9	**Erpresser-E-Mail 3 an Martin**

Stefan bemerkt schließlich, dass mit Martin etwas nicht stimmt, Martins Leistung fällt ab. Stefan spricht mit Martin, Martin bekennt sich als Opfer einer Erpressertat.	Monat 10	**Plakat** Mit Verantwortung! Helfen und helfen lassen!  *Abbildung 26 ML: Krimi – Helfen und helfen lassen*
(Rückblick)	Monat 11	**Plakat** „Informationssicherheit betrifft uns alle!“  *Abbildung 27 ML: Krimi – Informationssicherheit betrifft uns alle!*

Die Täterin gesteht die Tat!	Monat 12	**Verbrechervideo** Geständnis und Motive der Täterin  *Abbildung 28 ML: Krimi – Hackerin*

Weitergehende Erläuterungen bzw. eine ausführliche Anleitung stellt die Bundesakademie im Fortbildungsportal zum Download bereit, hier sind auch alle Medien abgebildet.

5.10 Zeitplan / Materialbestellung / Umsetzung

Wir unterstützen Sie bei der Umsetzung

Zeitplan

Um das Vorgehen bei der Planung und Durchführung der Sensibilisierungsinitiative in Ihrem Haus möglichst effizient zu gestalten, sollten Sie rechtzeitig Zeitpläne für die Umsetzung von Maßnahmen entwickeln. Bitte beachten Sie dabei, dass bei der Planung und Durchführung verschiedener (Kommunikations-) Maßnahmen ein dynamischer Prozess in Gang gesetzt wird, bei dem unterschiedliche Schritte ineinander übergehen oder parallel stattfinden könnten.

Abbildung 29 Fotolia: Kalender

So könnten beispielsweise zeitgleich zur Einführungsveranstaltung bereits Informationsmaterialien im Umlauf sein (z.B. Plakate), während vertiefende Workshops oder Seminare ggf. noch nicht komplett konzipiert sind und erst zu einem späteren Zeitpunkt umgesetzt werden. Das könnte zur Folge haben, dass Sie eine Maßnahme bereits auswerten, eine darauffolgende Maßnahme aber erst noch geplant werden muss.Achten Sie bei der Erstellung eines Projektplans deshalb immer darauf, ausreichend zeitlichen Spielraum für die Evaluierung und die Anpassung der Planung zu berücksichtigen.

Umsetzung

Um Sie bei der Umsetzung weiter zu unterstützen, haben wir Ihnen Checklisten zusammengestellt, mit deren Hilfe Sie sowohl den zeitlichen als auch organisatorischen Ablauf berücksichtigen können.

Die Checkliste verdeutlicht exemplarisch den chronologischen Ablauf bei der Umsetzung der einzelnen Kampagnenmaßnahmen. Es wird außerdem eine Verbindung zu den Instrumenten des BAköV-Werkzeugkastens hergestellt.

Auf Basis dieser Checkliste können Sie sich einen umfangreicheren Projektplan erstellen, mit dem Sie den Ablauf einer kompletten Sensibilisierungsinitiative planen können.

Material

Ihnen stehen Unterlagen, die wir Ihnen in „Teil II Der Werkzeugkasten“ vorgestellt haben, auf dem Fortbildungsportal zur Verfügung.

Wenn Sie Fragen haben sollten, wenden Sie sich bitte direkt an die BAköV.

5.11 Ihre Checklisten, ein Planungstool sowie eine Musterkampagne

Last but not least:

Als IT-Sicherheitsbeauftragte/r gehört die Organisation von Informationskampagnen nicht zu Ihrem täglichen Geschäft.

Wir unterstützen Sie daher mit Checklisten, die Ihnen sagen, wann Sie was unter Einbindung von wem organisieren sollten, damit „Sicher gewinnt!“ auch in Ihrem Haus ein Erfolg wird.

Abhängig von den (Kommunikations-) Maßnahmen, für die Sie sich entscheiden, können einzelne Vorbereitungen parallel laufen.

Die BAköV hilft Ihnen bei Fragen gern weiter.

5.11.1 Checkliste zur Vorbereitung von Sensibilisierungsmaßnahmen

	Aufgabe	**Wen einbinden?**	**Wann?**
1	Sie möchten in Ihrem Haus die Informationskampagne "Sicher gewinnt!" umsetzen. Entscheiden Sie zuerst, für wen in Ihrem Haus die Kampagne durchgeführt werden soll, mit welchen Schwerpunkten und welche Unterstützung Sie dafür benötigen: Nur Führungskräfte? Nur IT-Fachleute? Alle Beschäftigten? Arbeitsunterlagen: Arbeiten Sie jetzt mit den Moderationskarten, um Themen, Zielgruppen und Kommunikationskanälen zu bestimmen.	Direkt vorgesetzte Führungskraft, Behördenleitung, evtl. Personalabteilung, evtl. Bereich Öffentlichkeitsarbeit (ÖA), Personalvertretungen	Bei Beginn der Planungen

	Aufgabe	Wen einbinden?	Wann?
2	Nehmen Sie Kontakt mit der BAköV auf. Fragen Sie nach Möglichkeiten der Unterstützung für Schulungen, Vorführungen und Kommunikationsmaßnahmen. Hier erhalten Sie Informationen über mögliche Rahmenverträge etc. (weitere Infos unter www.bakoev.bund.de/sichergewinnt). Entscheiden Sie, ob in Ihrem Hause Informationsveranstaltungen z.B. mit Live-Hacking-Demonstrationen angeboten werden sollen. Eine Eröffnung durch die Hausleitung erhöht den Wert der Veranstaltung.	Direkt vorgesetzte Führungskraft, Behördenleitung BAköV lg5@bakoev.bund.de	Nach Entscheidung, in Punkt 1.
3	Informieren Sie sich über die vorhandenen Kommunikationsmedien zur Kampagne, die im BAköV-Werkzeugkasten online hinterlegt sind (https://lernplattform.intranet.bund.de). Entscheiden Sie, welche Medien zur Kommunikationskultur Ihres Hauses passen. Welche Medien sind für Ihre Zielgruppe (Führungskräfte, IT-Fachkräfte, alle Mitarbeitenden) geeignet?	Direkt vorgesetzte Führungskraft, Behördenleitung, evtl. Personalabteilung, evtl. Bereich ÖA, evtl. Personalvertretungen	Nach Bewilligung der Unterstützung durch die BAköV
4	Abstimmung über Schulungs- bzw. Veranstaltungstermine	Direkt vorgesetzte Führungskraft, Behördenleitung, evtl. Personalabteilung, evtl. Bereich Presse /ÖA, evtl. Personalvertretungen Extern mit BAköV evtl. einem externen Dienstleistungsunternehmen	Nach Bewilligung der Unterstützung durch die BAköV
5	Abruf der Kommunikationsmedien aus dem BAköV- Werkzeugkasten (z. B. Moderationskarten, Lernspiel, Plakate, Flyer, Informationstexte)		Nach Abstimmung über durchzuführende Veranstaltungen/Maßnahmen

	Aufgabe	**Wen einbinden?**	**Wann?**
6	Anpassung der Kommunikationswerkzeuge auf Ihr Behördenlogo (z.B. Plakate, Flyer, Informationstexte)	externe Dienstleistungsunternehmen	Nach Abstimmung über durchzuführende Veranstaltungen/Maßnahmen
7	Nutzen Sie die Ankündigungstexte zur Kampagne in internen Kommunikationsmedien (Intranet, Schwarzes Brett, Umlauf o. ä.). So bereiten Sie Ihre Kolleginnen und Kollegen auf den Start der Kampagne vor (Texte im Werkzeugkasten). Sollten Sie nur einzelne Zielgruppen ansprechen (Führungskräfte, IT-Fachkräfte), nutzen Sie die hierfür erstellten Texte zur persönlichen Ansprache).	Direkt vorgesetzte Führungskraft, die Behördenleitung, evtl. Personalabteilung, evtl. Bereich ÖA, evtl. Personalvertretungen	Sobald Ihnen die genauen Termine und Maßnahmen bekannt sind
8	Wenn Sie sich für Plakate entschieden haben: Beginnen Sie mit dem ersten Plakat (Ankündigung der Kampagne) gut eine Woche vor Start der Kampagne. Bereiten Sie Ihre Kolleginnen und Kollegen auf diese Weise auf die Kampagne vor und bringen Sie das Thema ins Gespräch. Geeignete Orte zur Plakatierung: Kantineneingang, Haupteingang, neben/in den Fahrstühlen, andere stark frequentierte Orte. Beim Druck der Plakate sind Ihnen Ihre Kolleginnen und Kollegen aus dem Bereich ÖA sicher gern behilflich. Alternativ können Sie die Plakate auch als PDF versenden. Achten Sie dabei bitte auf Barrierefreiheit.	Direkt vorgesetzte Führungskraft, die Behördenleitung, evtl. Bereich ÖA, Abt. Betriebsorganisation, Brandschutz	Sobald Ihnen die genauen Termine und Maßnahmen bekannt sind
9	Nutzen Sie die Flyer, um den Inhalt der Seminare/Schulungen/ Veranstaltungen zu vertiefen. Sie können die Flyer nach Abschluss der Veranstaltungen verteilen oder auch an prominenten Plätzen auslegen.	Direkt vorgesetzte Führungskraft, die Behördenleitung, evtl. Bereich ÖA, Abt. Betriebsorganisation, Brandschutz	Nach dem Start der Kampagne

	Aufgabe	Wen einbinden?	Wann?
10	Das Lernspiel „Quer durch die Sicherheit“ (S. 23) können Sie direkt bei der BAköV abrufen.	Direkt vorgesetzte Führungskraft, die Behördenleitung, evtl. Bereich ÖA, Abt. Betriebsorganisation	Nach dem Start der Kampagne
11	Zum Thema Bundes-Informations-Sicherheits-Schein (BISS) schauen Sie bitte ins Fortbildungsportal und wenden sich direkt an die Lehrgruppe 5 (lg5@bakoev.bund.de).	Direkt vorgesetzte Führungskraft, die Behördenleitung, evtl. Bereich ÖA, Abt. Betriebsorganisation	Nach dem Start der Kampagne
12	Evaluation: Prüfen Sie nach dem Abschluss der Kampagne die Nachhaltigkeit Ihrer Maßnahmen und ob Sie Ihre Ziele erreicht haben. Nutzen Sie dafür den eigens erstellten Fragebogen (s. Werkzeugkasten, „Teil I Der Sensibilisierungsleitfaden“). Starten Sie Umfragen, in welcher Weise das Thema Informationssicherheit und Datenschutz nach Abschluss der Kampagne in Ihrem Haus präsent ist. Die Ergebnisse stellen Sie bitte der BAköV zur Verfügung. Vielen Dank! Für die Bereitstellung von Mitteln sind der Vortrag bei der Behördenleitung sowie der Hinweis auf die Nachhaltigkeit und die Notwendigkeit der langfristigen Planung weiterer Maßnahmen sehr wichtig.	Direkt vorgesetzte Führungskraft, die Behördenleitung, evtl. Bereich ÖA, Personalvertretungen Abt. Betriebsorganisation	Nach Abschluss der Kampagne

Üben, üben, üben!

Beispiel PlanMICH Tafel mit Siggilinde

Siggilinde bekommt den Auftrag in ihrem Fachbereich eine kurze Bildungskampagne zum Thema „Informationssicherheit“ zu organisieren.

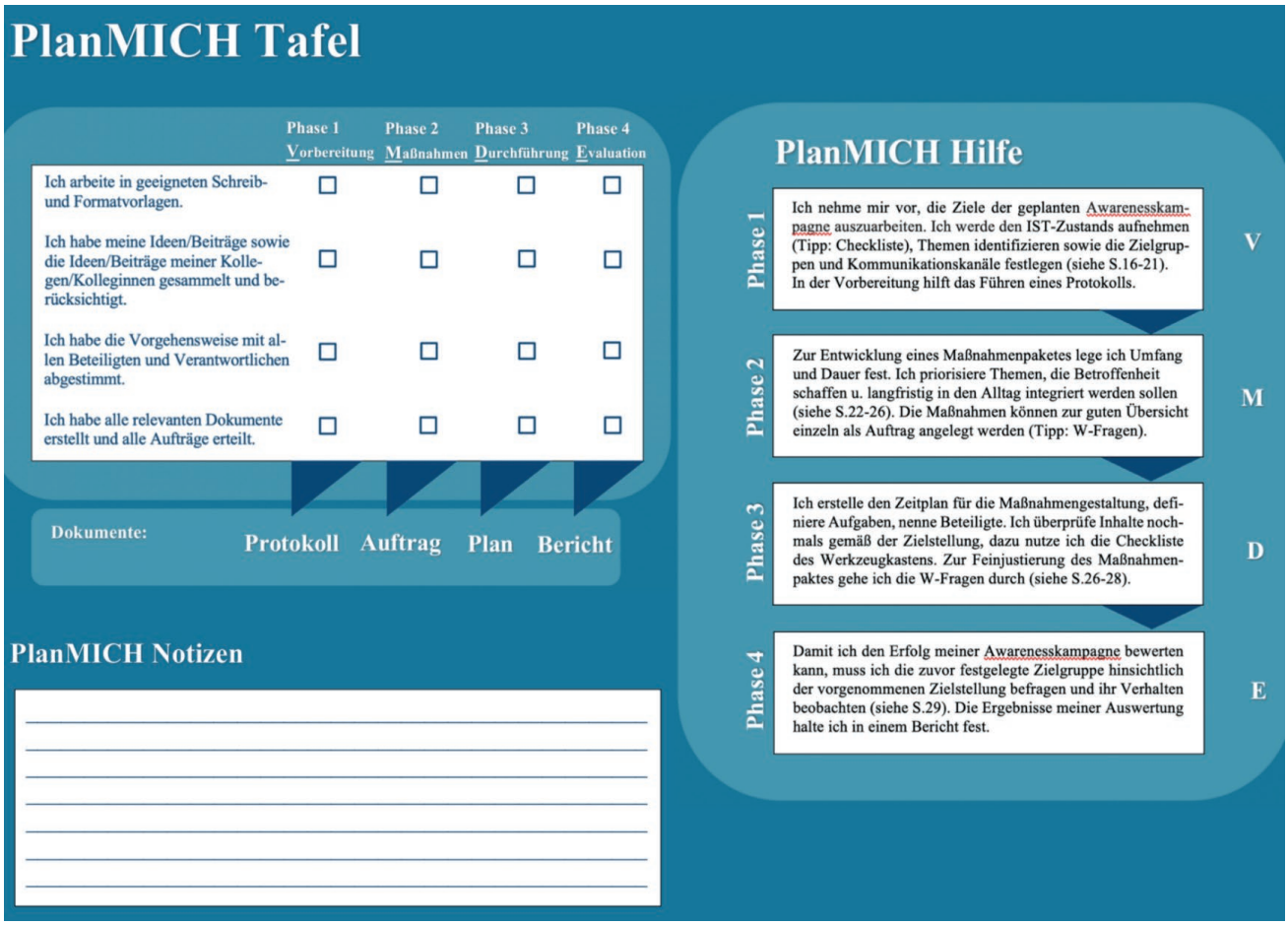


Abbildung 30 ML: PlanMICH

Beispiellösung

Siggilinde hat noch nie eine Kampagne organisiert und schaut deswegen in den Leitfaden „Sensibilisierung für die Informationssicherheit in der öffentlichen Verwaltung“. Sie findet als Hilfestellung die PlanMICH Tafel. Sie druckt die PlanMich Tafel in DIN A0 aus und hängt sie im Konferenzraum auf. Sie findet es gut, dass sie und andere die fortlaufende Fertigstellung des kleinen Projekts mitverfolgen können. Sie nimmt sich vor in den PlanMich Notizen die anstehenden Treffen mit ihrem Team festzuhalten.

Formatvorlagen und Umgang mit den relevanten Dokumenten

Siggilinde findet heraus, dass es für die Erstellung von Protokollen keine geeignete Formatvorlage gibt und erstellt für sich ein eigenes Dokument, in dem sie während des Entwicklungsprozesses der Kampagne fortlaufend die Fortschritte festhält. Sie unterscheidet im Protokoll zwischen ihren eigenen kreativen Prozessen, Terminen und Absprachen sowie Gesprächsergebnissen bei Abstimmungstreffen mit den anderen Verantwortlichen. Das Protokoll nutzt Siggilinde wie ein Arbeitsdokument, aus dem sie im Nachgang die weiteren Dokumente Auftrag, Plan und Bericht extrahiert. Für diese Dokumente behält ihre Behörde verschiedene Schreib- und Formatvorlagen vor. Sie setzt in ihrer PlanMich Tafel die ersten Häkchen:

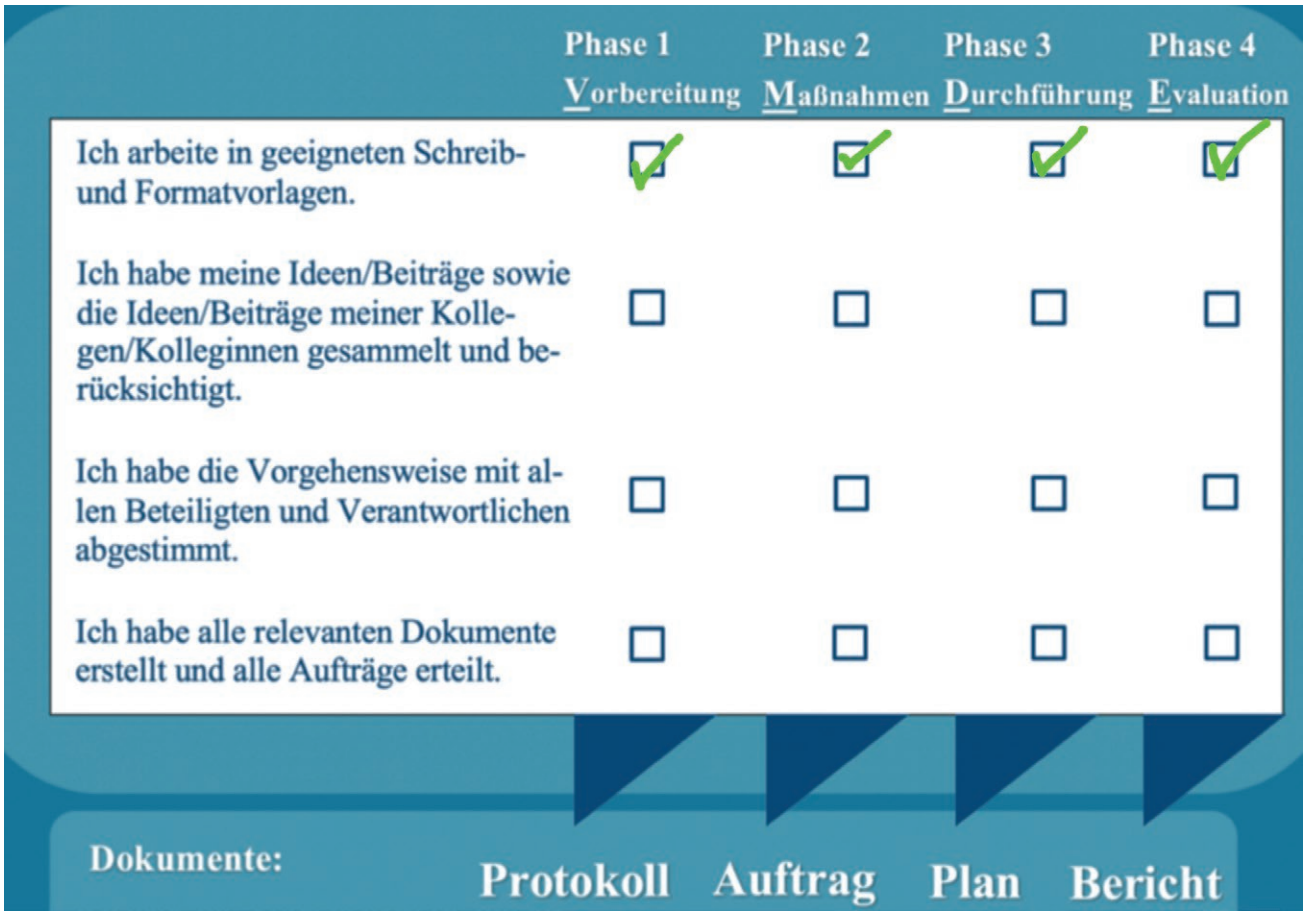


Abbildung 31 ML: PlanMICH 2

Die Zusammenarbeit mit Kollegen und Kolleginnen

Siggilinde und ihre Kollegen und Kolleginnen konnten erfolgreich die Ziele der Kampagne definieren. Auch die ersten Ideen zur Umsetzung von Maßnahmen, ein Workshop und die Erstellung von Plakaten haben sie besprochen. Siggilinde hat festgestellt, dass für alle Maßnahmen keine Unterstützung von Dienstleistungsunternehmen notwendig ist. Ihr Team kann auch die Produktion und Organisation der Maßnahmen selbst vornehmen. Sie hält alle Arbeitsergebnisse in ihrem Protokoll fest. Die Arbeitsgruppe hat festgelegt, dass sich zwei Gruppen zur inhaltlichen und organisatorischen Entwicklung der beiden Maßnahmen bilden. Siggilinde hat hierfür intern Aufträge erteilt und die Vorgehensweise auch mit ihrer Chefin abgestimmt. Sie setzt in ihrer PlanMich Tafel ihre Häkchen.

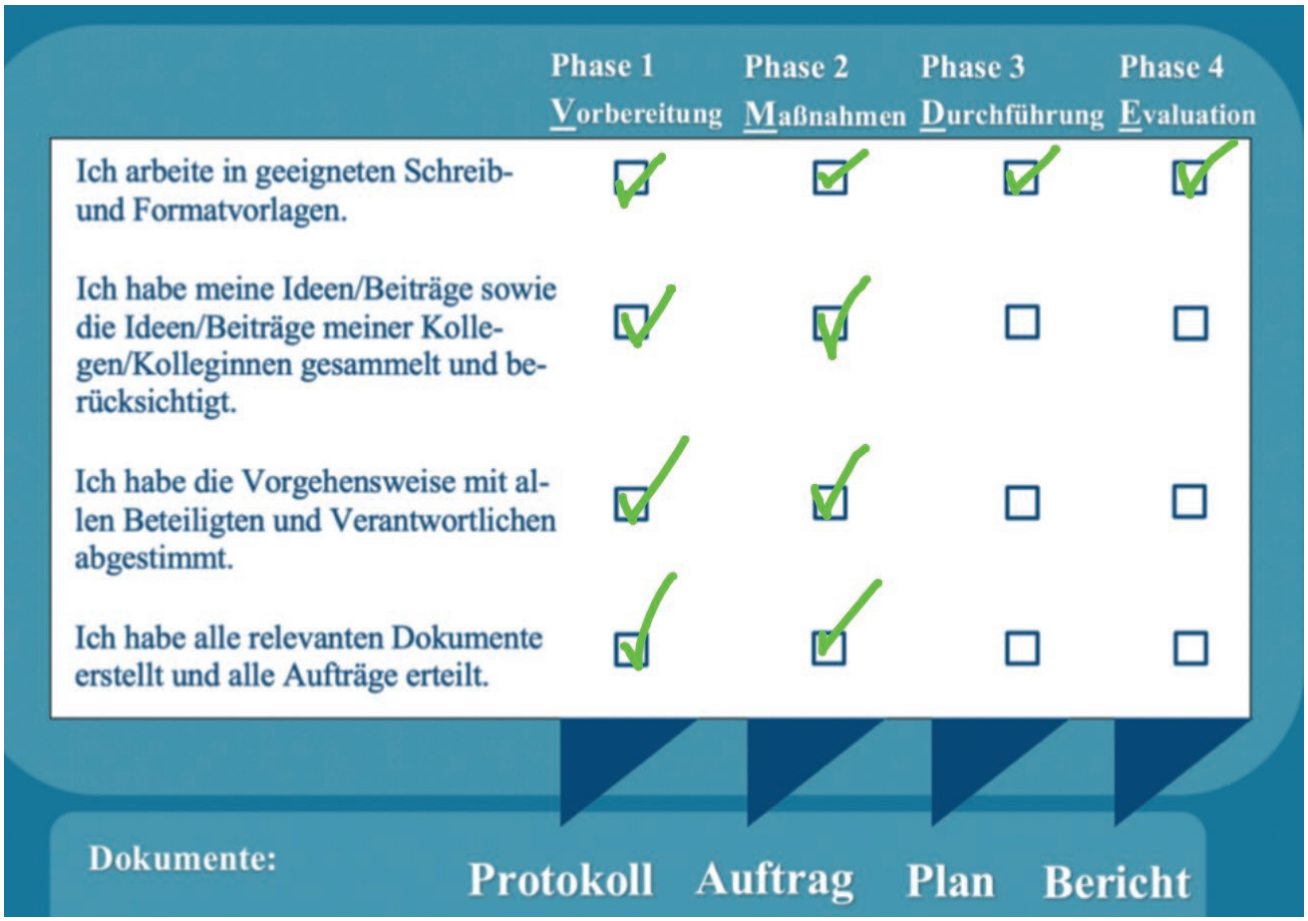


Abbildung 32 ML: PlanMICH 3

Nun stellt sie sich vor, wie die Kampagne durchgeführt werden könnte. Sie hält ihre Gedanken in ihrem Protokoll fest und datiert das nächste Treffen mit ihren Kollegen und Kolleginnen, um die Arbeitsergebnisse der beiden Gruppen „Workshop“ und „Plakate“ zu sammeln und gemeinsam zu besprechen.

Abbildung 33 ML: PlanMICH 4

Nutzung von Vorlagen: Der Werkzeugkasten

Die im Werkzeugkasten verfügbaren Konzepte und Vorlagen für Plakate, Flyer etc. wurden von Marketingfachleuten in Bezug auf Ausgestaltung, Design und Aussagekraft nach neuesten Erkenntnissen entwickelt und nach den Bundesregierungs-Corporate Design Regeln umgesetzt. Eine Verwendung in eigenen Maßnahmen ist ohne Probleme möglich, unterliegt aber folgenden einschränkenden Regeln:

- Das Behördenlogo darf nur an der dafür vorgesehenen Stelle eingesetzt werden.
- Farb-, Grafik-, und Layoutänderungen sind nicht gestattet.
- Zusätzliche Texte und Informationen sollten nur äußerst sparsam hinzugefügt werden.
- Druck wenn möglich nur in einer Druckerei, um optimale Ergebnisse, Farbbrillanz und Haltbarkeit zu erreichen.

5.11.2 Musterkampagne im Rahmen von „Sicher gewinnt“

Musterkampagne beim „frei erfundenen“ Bundesamt für künstliche Intelligenz (BAKI)

1. Ausgangslage: Ist-Situation, Übersicht über Maßnahmen und Projektbeteiligte aus vergangenen Jahren

Das Bundesamt für Künstliche Intelligenz hat zwei Standorte:

- den Hauptstandort Berlin mit 1.200 Beschäftigten,
- eine Forschungsabteilung mit 400 Stellen am Standort Sankt Augustin
- IT-Dienstleistungsunternehmen: ITZ Bund.

Der bisherige IT-SiBe hat die Behörde verlassen, der neue IT-SiBe steht jetzt vor der Herausforderung, erstmals eine Kampagne planen zu müssen. Der IT-SiBe möchte eine effektive und nachhaltige Kampagne planen. Hierzu stimmt er sich auch mit der Datenschutzbeauftragten im Bundesamt ab.

In 2015 hat es über den „Sicher gewinnt!“-Rahmenvertrag folgende Maßnahmen gegeben:

- Schulungen auf Basis des Standardseminares „Informationssicherheit und Datenschutz am Arbeitsplatz“ auf freiwilliger Basis.
- Live-Hacking-Veranstaltung auf freiwilliger Basis.
- Kurzfilmserie zu den „Goldenen Regeln“ aus dem Werkzeugkasten mit behördenspezifischem Vorspann wurde online auf freiwilliger Basis zur Verfügung gestellt.
- Ebenso wurde eine Sensibilisierung für die Führungskräfte durchgeführt und ein Sensibilisierungsworkshop für die IT-Beschäftigten.
- Broschüren und Flyer aus dem Werkzeugkasten sowie aus dem Angebot des BSI wurden in den Präsenzmaßnahmen verteilt.
- Plakate aus dem Werkzeugkasten wurden an gut frequentierten Stellen aufgehängt.
- Es wurde keine Evaluation zur Nachhaltigkeit und Effektivität der Maßnahmen durchgeführt.

2. Analyse und Bewertung der Ausgangslage, Ziele der neuen Kampagne 2021:

- An den Präsenzangeboten haben damals lediglich 30 Prozent der Beschäftigten teilgenommen.
- Seit 2015 sind etwa 30 Prozent neue Beschäftigte hinzugekommen, ebenso hat sich die Anzahl der Beschäftigten im Homeoffice deutlich erhöht.
- Daher müssen verstärkt digitale Angebote zur Verfügung gestellt und die neuen Beschäftigten sollen nach dem Wunsch der Behördenleitung verpflichtend geschult und sensibilisiert werden.
- Insbesondere aufgrund der Auswirkungen der Corona Pandemie muss auch über digitale Live Formate nachgedacht werden, z. B. über Webinare. Hierzu stellt die Bundesakademie für öffentliche Verwaltung über den Rahmenvertrag „Sicher gewinnt!“ die Plattform BigBlueButton zur Verfügung.
- Aufgrund der langen Zeit ohne Maßnahmen soll die neue Kampagne möglichst alle Beschäftigte erreichen.
- Insbesondere, weil in 2015 keine ausreichende Auswertung der Maßnahmen stattgefunden hat, soll dieses Mal eine möglichst umfassende Evaluation erfolgen.

3. Prüfung der verfügbaren Ressourcen und des Budgets

- Die Behördenleitung und Fortbildungsstelle des Bundesamts haben ihre Unterstützung zugesagt.
- Die Behördenleitung hat eine Budgetzusage gegeben und zugesagt, für die aktive Teilnahme an Veranstaltungen und sonstigen Aktionen zu werben.
- Da auch der administrative Datenschutz, der Geheimschutz und das Notfallmanagement des Bundesamts ähnlich gelagerte Maßnahmen planen, können Synergieeffekte genutzt werden (Budget, Ressourceneinsatz). Hier empfiehlt sich eine sehr enge Abstimmung bei der Maßnahmenauswahl.

Das vorhandene Budget ermöglicht es, ein externes Dienstleistungsunternehmen über den Rahmenvertrag „Sicher gewinnt!“ zur Unterstützung hinzuzuholen.

4. Nächste Schritte zur Projektinitiierung

1. Zusendung einer entsprechenden Bedarfsmeldung an die Lehrgruppe 5 der Bundesakademie für öffentliche Verwaltung, mindestens 4 Wochen vor Beginn der Maßnahmen
2. Abstimmung und Feinjustierung der Bedarfsmeldung mit dem Dienstleistungsunternehmen
3. Erstellung des Projektauftrags (2 Unterschriften zum Antrag an sich und zur Sicherstellung der HH-Mittel) mit umfassender detaillierter Beschreibung der einzelnen Projektmaßnahmen
4. Nach Unterzeichnung durch die BAköV und das Dienstleistungsunternehmen: Start der Kampagne im engeren Sinne

5. Kickoff Workshop zur Ausgestaltung der Kampagne

Durchführung mit dem Dienstleistungsunternehmen und verschiedenen Personen aus dem Haus (Datenschutz, Personalrat, IT, Gleichstellung, Notfallmanagement und Geheimschutz etc.).

Erarbeitung der Zielgruppen, der Kanäle und der relevanten Themen, sowie der daraus abgeleiteten Maßnahmen.

Mit den zur Verfügung stehenden Ressourcen werden folgende Maßnahmen geplant:

- Für alle Beschäftigten (inkl. Mobil-Arbeitende) wird verpflichtend die Bearbeitung der Lernwelt „Informationssicherheit und Datenschutz am Arbeitsplatz“ beschlossen.
- Ebenso soll der BISS-Test verpflichtend durchgeführt werden.
- Zwei kurze Veranstaltungen für die oberste Führung sollen angeboten werden, neben einem Vortrag soll es auch ein kurzes Planspiel geben. Aufgrund der Wichtigkeit sind vorab Pilotveranstaltungen geplant.
- Eine Teilnahme an einer an die Behörde angepassten Version des Standardseminares „Informationssicherheit und Datenschutz am Arbeitsplatz“ mit Aktiv-Komponenten soll angeboten und über die Führungskräfte „beworben“ werden.
- Kickoff in Berlin und Sankt Augustin: Es wird jeweils eine Großveranstaltung mit Hackern geplant, bei der die Kampagne nochmals angekündigt werden soll. Aufgrund der pandemiebedingten Lage in Bezug auf Großveranstaltungen werden die Veranstaltungen alternativ auch in einem digitalen Format konzipiert.
- In den Präsenzveranstaltungen soll, wie 2015, frei verfügbares Infomaterial (u.a. aus dem Werkzeugkasten) verteilt werden. Im Falle von digitalen Formaten muss die Verteilung auf anderem, digitalem Wege erfolgen.
- Standardplakate aus dem Werkzeugkasten sollen ebenfalls die Kampagne bewerben.
- Angebot des BAköV-Krimis „DenkXsicher“ und den entsprechenden Informationsträgern.
- Diese werden über einen Zeitraum von zwölf Monaten über die neu zu erstellende Kampagnen-Intranetseite zur Verfügung gestellt.
- Über zusätzliche Ressourcen kann ein kurzes, individuelles E-Learning erstellt werden, welches die Lernwelt um die Spezifika des Standardseminares ergänzt.
- Um den aktuellen Stand der Awareness vor dem Kampagnenstart in der Behörde festzustellen, werden die Beobachtungen und Erkenntnissen der IT und der Beauftragten ausgewertet, ebenso wird über das Intranet eine Befragung der Beschäftigten initiiert
- Im Rahmen der Evaluation und der Erstellung des Nachhaltigkeitskonzepts für die kommenden Jahre soll diese Vorgehensweise wiederholt werden. Weiterhin sollen dann die Erkenntnisse aus der Bearbeitung des Krimis sowie dessen Akzeptanz generell ausgewertet werden.

- Generell, aber auch besonders aufgrund der aktuellen Lage, wird ein besonderer Wert auf ein flexibles Changemanagement gelegt. Deshalb sind nicht nur alternative Formate, siehe oben, sondern es wird auch eine Zwischenevaluation eingeplant, nach der alle Maßnahmen nochmals auf ihre Wirksamkeit überprüft werden.

Am Ende wird ein Zeitplan erstellt und die durchzuführenden Maßnahmen werden in eine methodisch-didaktisch zielführende und auf die sonstigen Rahmenbedingungen abgestimmten Reihenfolge gebracht, woraus der „Kampagnenfahrplan“ folgt, siehe Anlage, grafische Darstellung.

6. Durchführung: Vorbereitende Maßnahmen

- Hierzu wird auf den oben angesprochenen Kampagnenfahrplan aufgesetzt.
- Durchführung einer Erstevaluation. Dazu werden Befragungen im Intranet sowie Einschätzungen der IT-Abteilung und des Sicherheitsmanagements ausgewertet und exemplarisch Interviews durchgeführt. Es werden kleinere Tests konzipiert und im Intranet bereitgestellt.
- Auswertung der Ergebnisse, die wiederum in die Kampagne sinnvoll integriert werden.
- Anpassung des Konzepts zum Standardseminar, Erstellung der Präsentation, Einarbeitung der internen Regelungen und Richtlinien, Berücksichtigung der Anforderungen von Datenschutz, Geheimschutz und Notfallmanagement.
- Mit dem Dienstleistungsunternehmen wird das Drehbuch für das angepasste E-Learning erstellt.
- Begleitunterlagen werden erstellt; diese sollen während der Präsenzveranstaltungen verteilt werden, oder bei Onlineformaten digital versendet werden.
- Die Plakate werden angepasst, eine spezielle Intranet-Kampagnenseite wird mit eigenen Mitteln aufgebaut. Hierüber wird u. a. auch der BISS, die Lernwelt, der Krimi, das individuelle E-Learning sowie auch weiteres digitales Material angeboten.

7. Durchführung im engeren Sinne:

- Die Kampagnenseite wird publiziert.
- Alle Maßnahmen werden gemäß Kampagnenfahrplan durchgeführt. Zwischenevaluationen begleiten die Durchführung. Mit einer zweiten Evaluation endet zunächst die Kampagne 2021 – 2022.

8. Evaluation:

- Berücksichtigung des Ergebnisses des Krimis, dazu Beobachtungen und Erfahrungen der IT-Sicherheits-, Datenschutz- und Geheimschutzbeauftragten sowie der IT-Abteilung (u.a. Interviews, Anrufe beim Benutzerservice, Besuche auf der Intranetseite etc.)
- Auswertungen per Evaluationsbögen aus den Präsenzschulungen/Onlineformaten, Erkenntnissen des IT-Dienstleistungsunternehmen bzw. der Hotline.
- Erstellung eines Evaluationsberichts zusammen mit dem externen Dienstleistungsunternehmen für die BAköV.

- Dieser Bericht dient auch als Nachweis für die Durchführung von Sensibilisierungsmaßnahmen zu anderen Zwecken (Bundesrechnungshof, Sachstandsbericht UP Bund 2017 etc.).
- Ebenso wird daraus ein Nachhaltigkeitskonzept generiert, welches der Behördenleitung zur Abstimmung des Sensibilisierungsbudgets für die kommenden Jahre vorgelegt wird.
- Im Sinne des PDCA-Zyklus sollten kleinere Maßnahmen (z.B. die Informationsträger aus dem Krimi) als Wiedererkennung losgelöst von der vorstehenden Gesamtkampagne hin und wieder nochmal verwendet werden.
- Aufgrund einer potenziellen Desensibilisierung sollte frühestens in 2025 wieder eine neue Kampagne im Bundesamt durchgeführt werden.
- Für zwischenzeitliche Neueinstellung empfiehlt sich davon unabhängig in jedem Fall stets die Lernwelt und der BISS.

9. Kampagnenfahrplan (Beginn 06.2021 Grafische Darstellung)

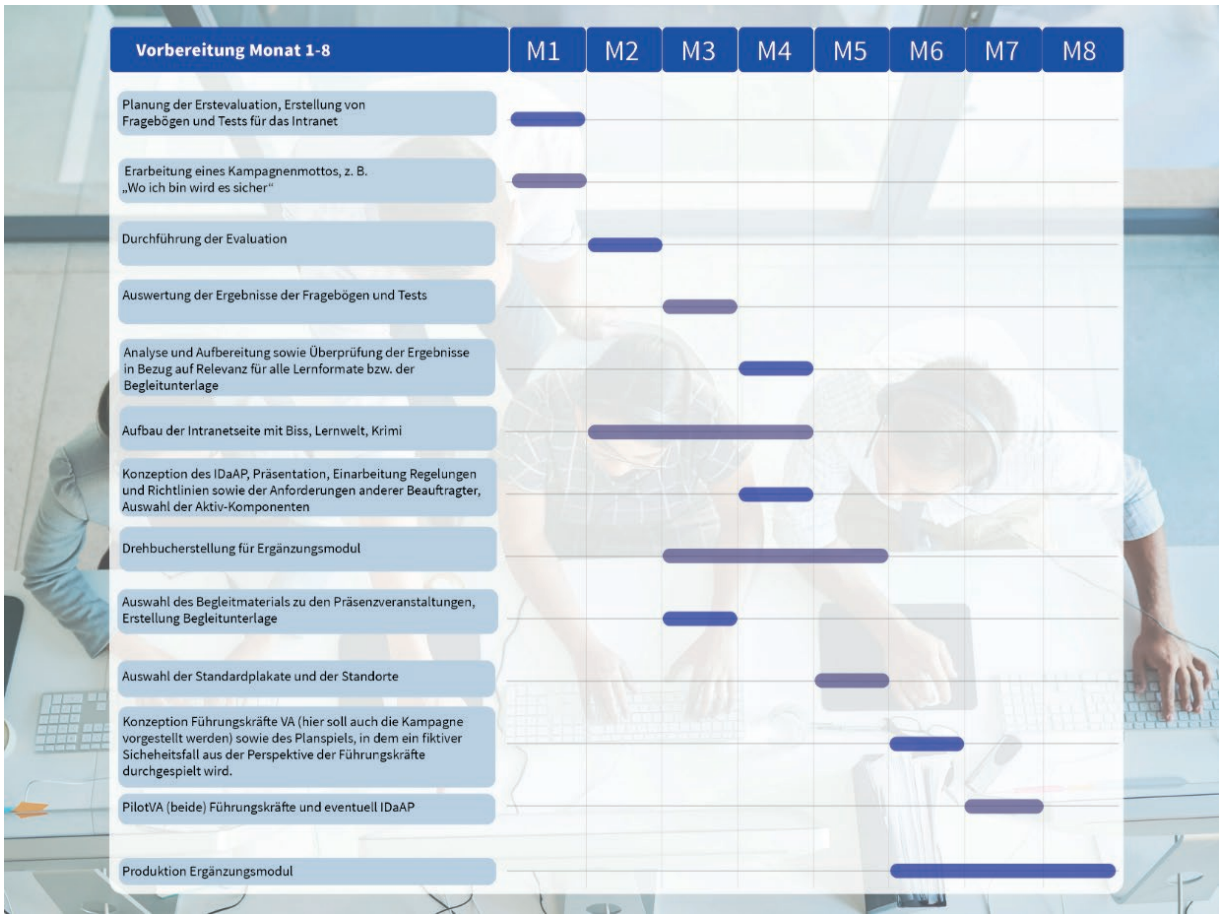


Abbildung 34 ML: Fahrplan 1

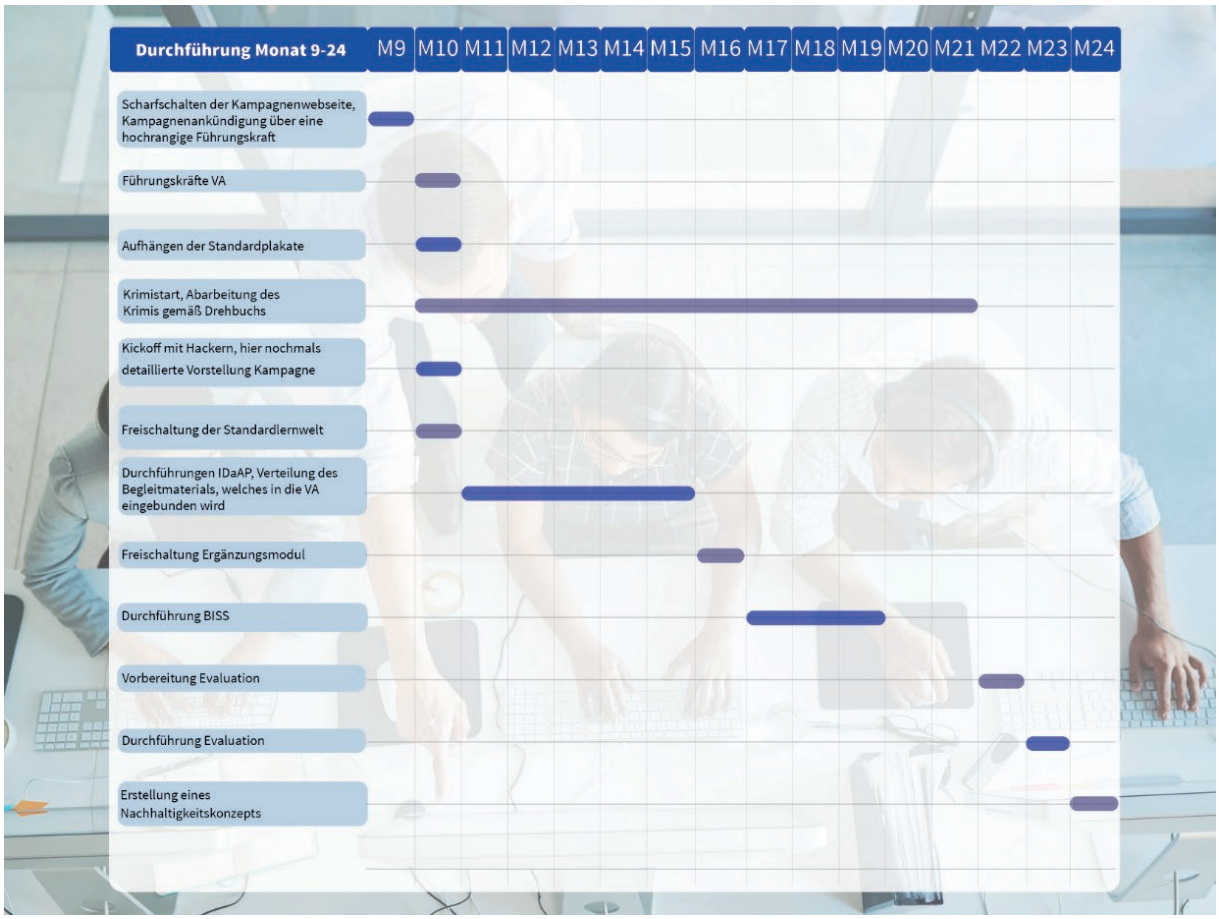


Abbildung 35 ML: Fahrplan 2

6. Exkurs:

6.1 Kommunikation und Ansprache

Es ist wenig Erfolg versprechend, bei den Beschäftigten durch Zwänge oder Überredungskünste ein Bewusstsein für die Notwendigkeit von Informationssicherheit zu bilden. Stattdessen sollten folgende Prinzipien umgesetzt werden:

- **Positive Kommunikation:**

Eine Sensibilisierung wird am ehesten erreicht, wenn eine positive Haltung eingenommen und über Fehlverhalten, Irrtümer oder gefährliche Stressreaktionen ohne Vorwurf kommuniziert wird. Nur so kann ein partnerschaftlicher Dialog etabliert werden, der die Beschäftigten zu Verbündeten bei der Durchführung von Informationssicherheitsmaßnahmen macht und ihnen die Chance einräumt, eigene Vorschläge oder Anmerkungen einzubringen. Die Rolle der Beschäftigten (Pflichten und Aufgaben innerhalb Ihrer Behörde) sollte in die Zielstellungen einfließen und geklärt werden, wie sie für eine positive Auseinandersetzung (Multiplikatoren) mit dem Thema Informationssicherheit gewonnen werden können.

- **Die Schockwirkung:**

Die ausgewählten Maßnahmen sollten die Mitarbeitenden „wachrütteln“, nicht aber in Angst oder Unsicherheit versetzen. Oft ist dies ein schmaler Grat. Eine Trick-Mail mit gefälschten Links oder ausführbaren Anhängen angelehnt an eine typische Angriffsmail sollte auf positive Art den gemachten Fehler erläutern. Sie sollte jedoch nicht dazu führen, dass z. B. der Bildschirm schwarz wird oder der Rechner sich ausschaltet. Dies würde die Beschäftigten in Bedrängnis bringen und nicht die gewünschte positive Einstellung zur Kampagne erzielen. Es könnte sogar kontraproduktiv dazu führen, dass gar keine Links oder Anhänge mehr genutzt werden. „Wecken“ – nicht „erschrecken“ – sollte daher bei allen Maßnahmen das Motto sein.

- **Wissen durch Information:**

Informationen sollten auf informative und unterhaltsame Art und Weise und ohne Belehrung vermittelt werden. Möglichst alltagstaugliche Beispiele helfen bei der Veranschaulichung und bilden die Voraussetzung dafür, dass die Belegschaft für den Zusammenhang zwischen eigenem Handeln und möglichen Konsequenzen sensibilisiert wird.

- **Motivation zur Eigenverantwortung:**

Eigenverantwortung und persönliches Engagement der Beschäftigten sollten unterstützt werden. Informations- oder Schulungsangebote setzen Anreize für die Themen und ermutigen Sie sie dazu, gewonnene Kompetenzen auch einzusetzen und anderen bei Bedarf zu helfen. Die lobende Kommunikation („Wir haben es gemeinsam geschafft“) positiver Entwicklungen, wie eine verbesserte Sicherheitslage, wird als Erfolgserlebnis empfunden und steigert die Bereitschaft, das eigene Verhalten weiter zu verbessern.

- **Kompetenz durch Training**

Regelmäßige Wiederholungen, besonders von Grundkompetenzen wie dem Lesen von URL und Erkennen von E-Mail-Adressen können helfen stereotypes „sicheres“ Verhalten zu fördern.

7. Impressum

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

Tel. 0228 99629-0
E-Mail: lg5@bakoev.de

Inhalt/Texte:
secunet, Security Network AG www.secunet.com
ML Gruppe, ML Consulting www.mlgruppe.de

Februar 2021

Bildnachweise