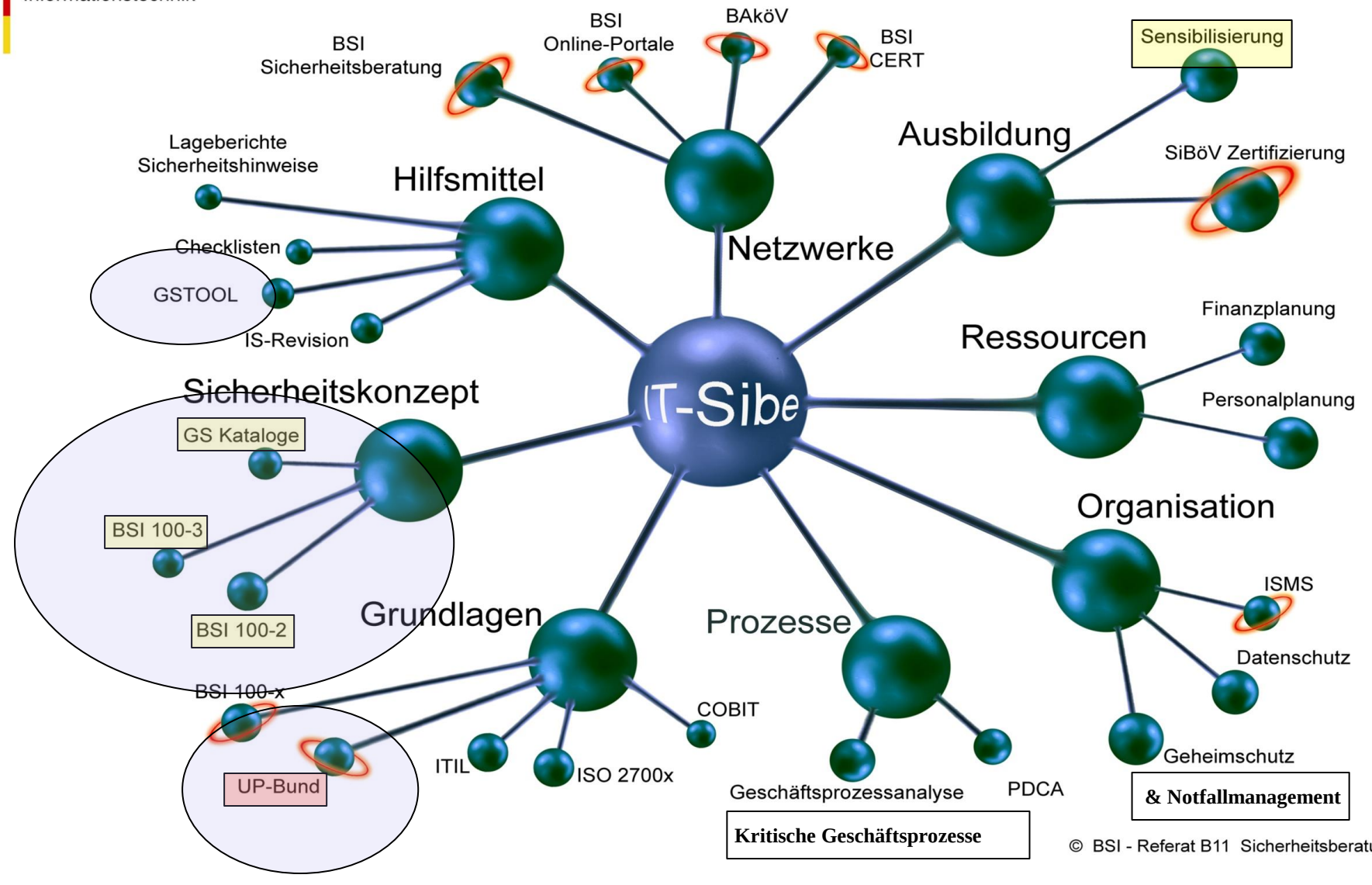
Bundesministerium des Innern

Neues aus der BAköV Fortbildung
IT-Sicherheit und Sensibilisierung 2016/17

IT-Sicherheitsbeauftragte öffentliche Verwaltung

Bundesministerium des Innern

Bundesamt
für Sicherheit in der
Informationstechnik



Gefährdungslage	Technische Entwicklung	Digitale Verwaltung e - xxxxx	IT Konsolidierung

Fortbildung Digitalisierung der Verwaltung

IT 205 /17	Besondere Rahmenbedingungen für IT-Projekte in der Bundesverwaltung
IT 210 /17	IT-Projektmanagement Aufbau
IT 211 /17	Erfahrungsaustausch für IT-Projektleiter
IT 212 /17	Agiles IT-Projektmanagement am Beispiel von Scrum

IT 310 /17	Digitale Verwaltung in der Praxis - Grundlagen - IT-gestützte Vorgangsbearbeitung, Prozessoptimierung und Dokumentenmanagementsystem -
IT 315 /17	Digitale Verwaltung in der Praxis - Aufbau - Methoden und Techniken der Geschäftsprozessoptimierung zur Einführung IT-gestützter Vorgangsbearbeitung -

Fortbildung IT-Konsolidierung

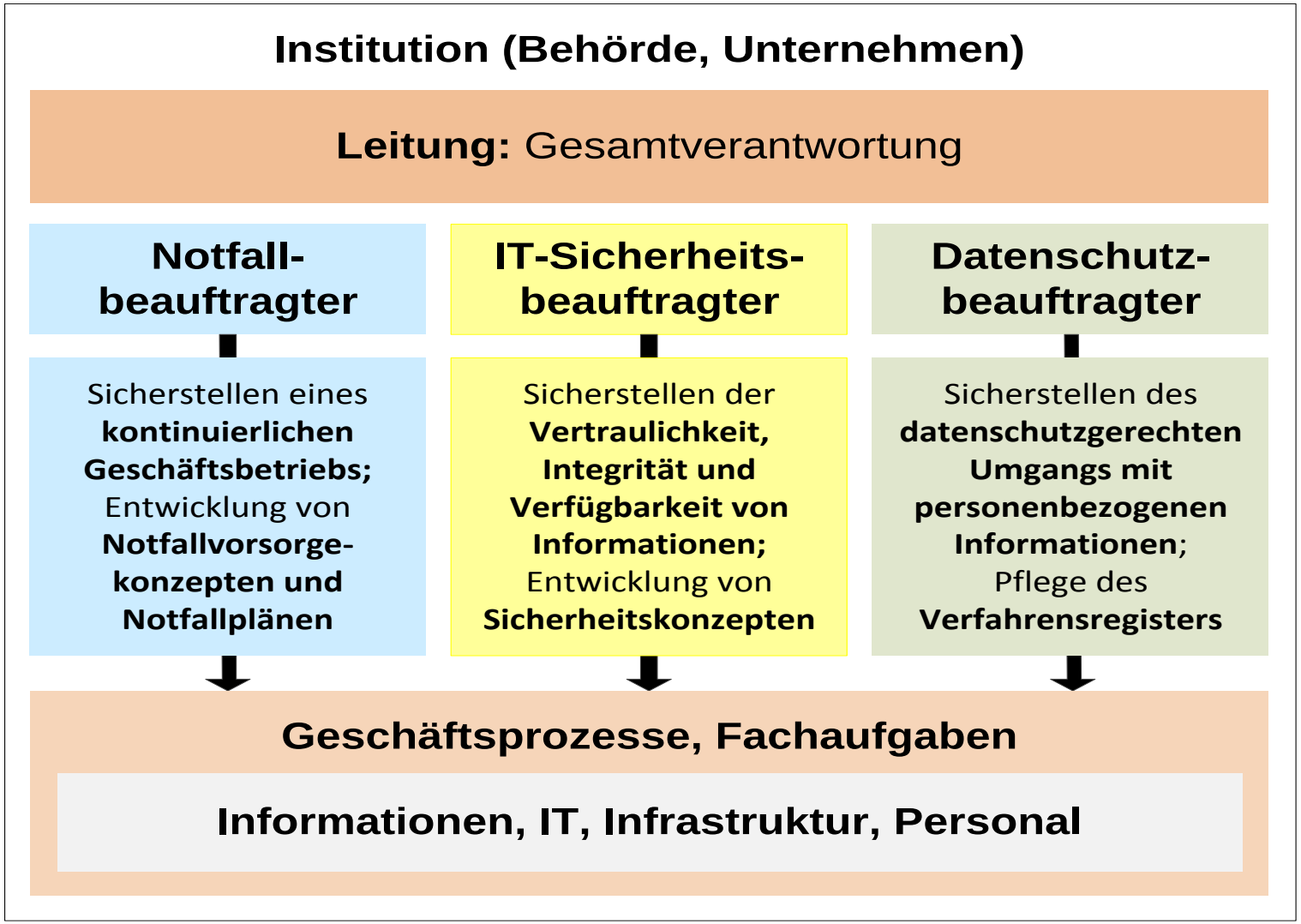
IT 150 /17	IT Konsolidierung - Anforderungen an die Kundenbehörde
IT 250 /17	Standard zur Gestaltung von IT Service Prozessen - unter Nutzung von ITIL V3 (IT Infrastructure Library)
IT 255 /17	Implementierung von IT Service Management nach ITIL in der öffentlichen Verwaltung
IT 213 /17	Fachübergreifende Kommunikation in IT-Projekten - Kommunizieren zwischen IT- und Verwaltungskräften -

Fortbildung Technische Entwicklung

IT 430 /17	Verschlüsselung und Elektronische Signatur
IT 465 /17	Unterstützung des IT-Grundschutz mit Tools
IT 600 /17	Grundlagenwissen für Systemadministratoren in der öff. Verwaltung
IT 604 /17	Einstieg in Linux
IT 605 /17	Vertiefung Windows Netzwerke
IT 606 /17	Vertiefung Linux/UNIX Netzwerke
IT 607 /17	IT-Sicherheitsaspekte in heterogenen Netzen
IT 610 /17	SQL - Die Abfragesprache für Datenbanken
IT 616 /17	Betrieb von E-Mail-Servern - am Beispiel von MS Exchange
IT 630 /17	Daten- und Informationssicherheit beim Einsatz mobiler Geräte
IT 660 /17	Steuerung und Organisation des IT-Supports
IT 680 /17	Computer-Forensik in Theorie und Praxis

Übungszentrum Netzverteidigung der BSI
Datum : 05.12.2016 bis 09.12.2016
Ort: BAköV in Brühl

- Grundlagen Hacking und Verteidigung
- Angriffe auf das Netzwerk, korrespondierende Sicherheitsmaßnahmen
- Angriffe auf Clients, korrespondierende Sicherheitsmaßnahmen
- Angriffe auf ICS / SCADA-Umgebungen, korrespondierende Sicherheitsmaßnahmen
- Angriffe auf Mail Applikationen, korrespondierende Sicherheitsmaßnahmen
- Angriffe auf Web Applikationen, korrespondierende Sicherheitsmaßnahmen


Institution (Behörde, Unternehmen)
Leitung: Gesamtverantwortung
Notfall-beauftragter
IT-Sicherheits-beauftragter
Datenschutz-beauftragter
Sicherstellen eines kontinuierlichen Geschäftsbetriebs; Entwicklung von Notfallvorsorge-konzepten und Notfallplänen
Sicherstellen der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; Entwicklung von Sicherheitskonzepten
Sicherstellen des datenschutzgerechten Umgangs mit personenbezogenen Informationen; Pflege des Verfahrensregisters
Geschäftsprozesse, Fachaufgaben
Informationen, IT, Infrastruktur, Personal

Fortbildung IT-Sicherheitsbeauftragte - Aufbau- NEU

IT 489/17

- Modernisierung des IT-Grundschutzes – Von Anforderungen zu Maßnahmen
- Identifikation und Bewertung von Risiken
- Herausforderungen bei IT-Projekten insbes. Digitalisierung
- Informationssicherheit bei der IT-Konsolidierung
- Anforderungen Outsourcing und Steuerung externer Dienstleister
- Cloud Sicherheit
- Verfahren und Modelle zum Messen und Bewerten des Reifegrades der Informationssicherheit
- etc.

Beauftragte Notfallmanagement – Datenschutz - Geheimschutz

IT 410 /17	Sensibilisierungskampagnen und Schulungen in IT-Sicherheitsfragen - Konzeption und Durchführung

BF 500 /17	Notfallmanagement etablieren, umsetzen und steuern
BF 505 /17	Vertiefungsseminar zum Notfallmanagement - Business Impact- und Risikoanalysen
BF 510 /17	Erfahrungsaustausch für Notfallbeauftragte

IT 417 /17	Materieller und IT-Geheimschutz - In Zusammenarbeit mit dem BSI -
IT 418 /17	Grundlagenwissen für VS-Verwalter - In Zusammenarbeit mit dem BSI -

Beauftragte Notfallmanagement – Datenschutz - Geheimschutz

BF 210 /17	Datenschutz und Datensicherheit
BF 220 /17	Schutz von Personaldaten - Rechtliche Grundlagen –
BF 250 /17	Behördliche Datenschutzbeauftragte in der Bundesverwaltung
SO 522 /17	Die EU Datenschutz-Grundverordnung 2016
BF 320 /17	Das Informationsfreiheitsgesetz des Bundes

Fortbildung übergreifend

SO 203 /17	Jahrestagung für behördliche Datenschutzbeauftragte in der Bundesverwaltung
SO 500 /17	Sommerakademie für Landes- und Kommunalbedienstete - IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I - Basis -
SO 505 /17	Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden
<u>Workshopreihen</u> SO 506 /17	für IT-Sicherheitsbeauftragte
SO 520 /17	für behördliche Datenschutzbeauftragte in der Bundesverwaltung
SO 560 /17	für Beschäftigte im IT-Bereich
SO 570 /17	für IT-Beschaffer

Sensibilisierung Informationssicherheit

Bundesministerium
des Innern

Informationssicherheit in der Bundesverwaltung
„Sicher gewinnt!“ 2010 bis heute

Ergebnisse Diplomarbeit Linda Streppelhoff

Vorher:

- Sensibilisierung in Informationssicherheit war in 57,1% der befragten Behörden der Mehrheit der Mitarbeiter völlig unbekannt

- Der Erfolg der Sensibilisierungsmaßnahmen wurde in 90,5% der Fälle positiv bewertet.

- mehr als 50% bis 80 % der Beschäftigten wurden erreicht

- neue Mitarbeiter werden beim Eintritt in die Behörde zum Thema Informationssicherheit geschult => Nachhaltigkeit

Awareness herstellen!

- Wissen
- Wollen
- Können

Kompetenz ist Handlungswissen

Im 7. Jahr

Das Projekt „Sicher gewinnt!“

- Sensibilisierung von Bundesbeschäftigten im Umgang mit Informationssicherheit am Arbeitsplatz, zusammen mit BSI
- 160 Behörden, ca. 150.000 Beschäftigte
- basierend auf dem Leitfaden „Sicher gewinnt!“

NEU!!

FAZIT

1.) Sensibilisierung

ist ein Thema, welches immer wieder neu aufgegriffen werden muss

2.) Zentral steuern – dezentral umsetzen – dezentral anpassen

3.) Rahmenverträge haben sich bewährt

4.) Der Werkzeugkasten

Sensibilisierung und Schulung- Start

- Vorgehensweise nach Leitfaden hat sich bewährt
- Erfassung der Situation, Zielgruppen und Inhalte durch Interviews im IT-Sicherheitsmanagement, mit der Hotline, der IT-Leitung
- Umsetzung mit der Hausleitung und deren Sensibilisierung wichtig
- Vielfältige Wege –Nutzung Intranet, Schulungen

Fazit - Erfolgreiche Awarenessinitiativen haben

- ein **Ziel** formuliert
- ein **Vorgehen** vereinbart, nutzt die Kapazitäten der Fortbildungsstelle
- einen Zuschnitt auf die **Behördenkultur**
- Die Unterstützung der **Behördenleitung**
- **verzahnte Einzelmaßnahmen**
- eine verbindende **Klammer**

Wie wird der Prozess der Sensibilisierung fortgesetzt?

Gibt es Erfahrungen?

Soll der Rahmenvertrag nach 2017 neu aufgesetzt werden?

Was erwarten Sie vom Dienstleister

Zentral steuern und anbieten

Erfahrungen : Branding

SIGGI SICHER und SIGGILINDE

Sympathieträger für Sensibilisierungsmaßnahmen in der Bundesverwaltung

Der Werkzeugkasten
Neu

www.lernplattform-bakoev.bund.de

WERKZEUGKASTEN für Landes- bzw. Kommunalverwaltungen

Hier finden Sie Werkzeuge zur Planung, Durchführung und Evaluation von Sensibilisierungs- und Schulungsmaßnahmen.

Neues Objekt hinzufügen

Ordner

- **Planung und Bedarfsermittlung**
  Erste Schritte zur eigenen IT-Sensibilisierungskampagne ...
- **Ankündigung der Kampagne**
  Bereiten Sie die Umsetzung der Kampagne vor - wir stellen Ihnen die Texte zur Verfügugung. Die Werbemedien finden Sie unter...
- **Gedruckte Medien**
  Plakate, Flyer und Broschüren, Bilder, Logos und Comics - hier finden Sie alle Druckunterlagen.
- **Digitale Medien**
- **Veranstaltungen vor Ort**
- **Siggi Sicher**
  Maskottchen der IT-Sensibilisierungskampagne
- **Evaluation**
  Und? Wie war's? ...
- **Der BISS**
  Hier finden SIe Plakatvorlagen und den Flyer zum Bundes-Informations-Sicherheitsschein.

Medienpools

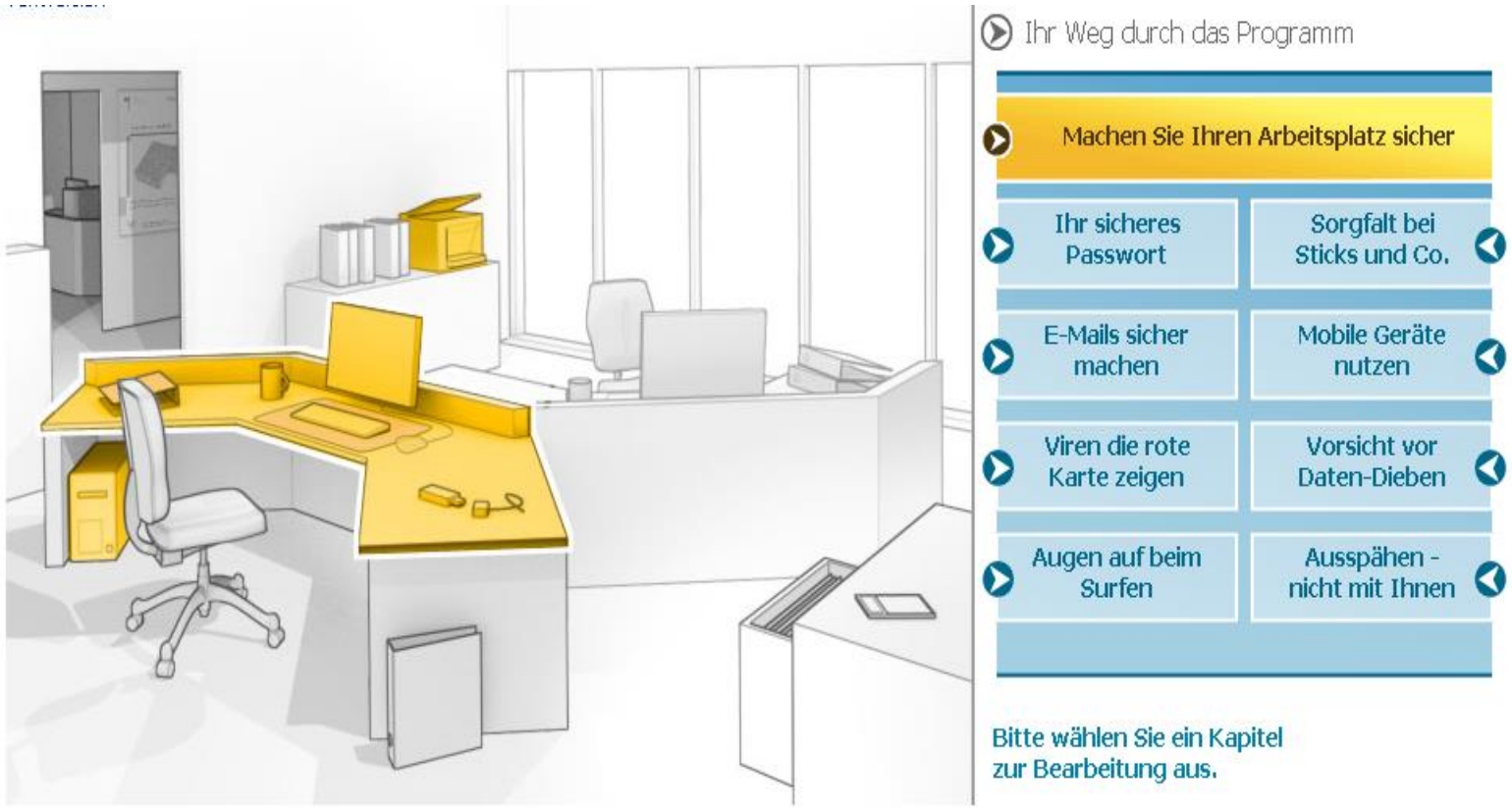
- **Medien zur IT-Sensibilisierungskampagne**

Schulung „Informationssicherheit am Arbeitsplatz“ NEU!

Feinkonzept, Skript und Module

- Smartphones
- Datenschutz
- Mobile Computing
- **Social Engineering**
- Passwörter
- Weitergabe von Daten
- Aktuelle Maleware-Trends
- Online Kriminalität
- Dienste im Dienste
- Soziale Netzwerke
- Cloud Dienste

Lernwelt „Informationssicherheit am Arbeitsplatz“
Neu 2015 und Kalender 2017



Der Werkzeugkasten – Die Plakate und Bilder NEU

- Plakate Serie Fotos und Flyer
- Plakate Serie Comics
- Plakate Serie Lernwelt
- Tipps für Jedermann


Bitte setzen Sie hier Ihr Behördenlogo ein.
Am <Datum> um <Uhrzeit> in <Ort> Anmeldung unter <Adresse>
Einladung zum IT-Sicherheitstag
Tragen Sie hier die Highlights Ihrer Veranstaltung ein.


Bundesministerium des Innern
Scharfschließen
Schützen Sie Ihre Daten!
Achtung: Verschließen Sie Ihre Dateien, Ihre Schränke und Ihre Tür, wenn Sie nicht am Arbeitsplatz sind.


Bitte setzen Sie hier Ihr Behördenlogo ein.
Große Lauscher
Sie sind in Ihr Gespräch vertieft. Wer noch?
Achtung: Vermeiden Sie Gespräche mit sensiblem Inhalt in der Öffentlichkeit. Sie wissen nie, wen es noch interessieren könnte.

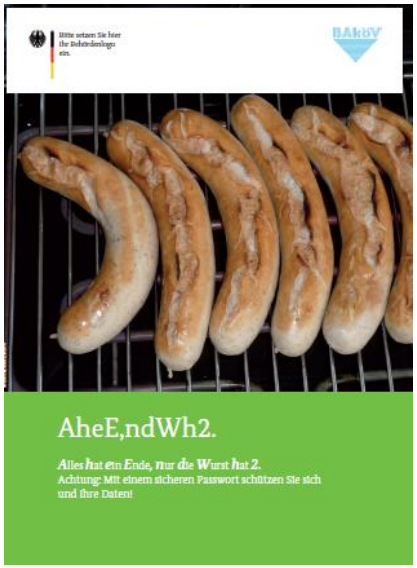

Bitte setzen Sie hier Ihr Behördenlogo ein.
Tipps für mehr Informationssicherheit
So schützen Sie sich und unser Haus vor Cyberangriffen.

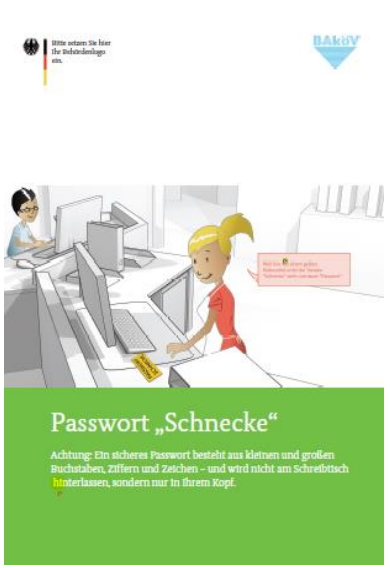

Bitte setzen Sie hier Ihr Behördenlogo ein.
Hallo.
Achtung Datendiebe!
Lassen Sie sich nicht aushorchen!
Behalten Sie Ihre Passwörter, personenbezogene Daten und andere sensible Informationen für sich.


Nicht alle Fälschungen sind offensichtlich
Vorsicht bei E-Mails!
IT-Sicherheit im Fokus

Thema: Passwortsicherheit

Bundesministerium des Innern | Bundesamt für Sicherheit in der Informationstechnik





Bundesministerium des Innern

BISS - Aktualisierung 2015

Wer hat den BISS gemacht?

Foto: R_by_ww/PIXELIO

Der Bundes-Informationssicherheits-Schein (BISS)
auf www.lernplattform-bakoev.bund.de

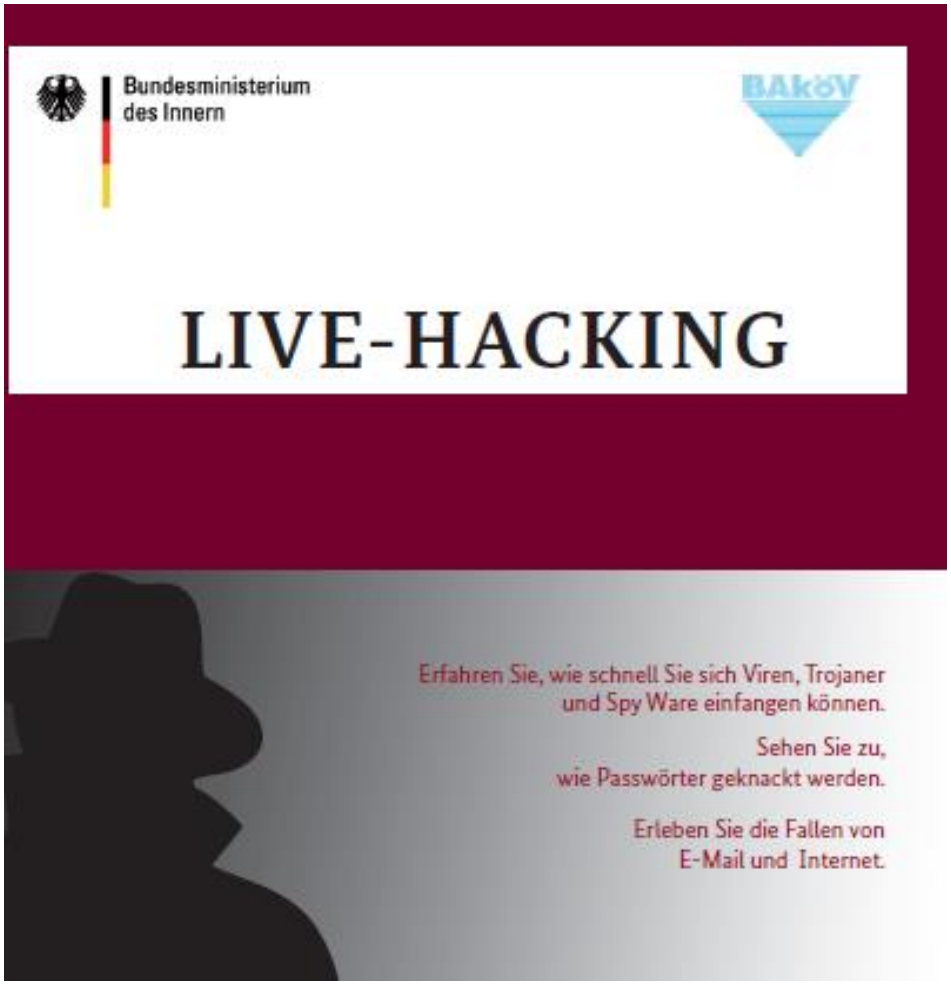
Nähere Informationen finden Sie
im Intranet

Bundesinformations-Sicherheits-Schein

- Onlinetest
- 15 Fragen
- Bearbeitungszeit 15 Minuten
- Zertifikat

Die Roadshow 2011 - 2015
Angebot für Bund und Länder

2015
Neue Veranstaltung
und DVD



Angebot
Evaluation

Evaluation mit der Lernplattform

Domäne/ Bereiche	Zentraler Aspekt
Arbeits- und Technologiegestaltung	Wie gestaltet die Behörde den Umgang mit der Technologie und den Arbeitsprozessen?
Personalwesen	Übernimmt die Personalsbteilung ihre Aufgabe im Bereich Informationssicherheit?
Organisationskultur	Wie ist der zwischenmenschliche Umgang im Unternehmen?
Organisationsstruktur	Wie ist die Informationssicherheit organisiert?
Kommunikation	Wie ist die innerbehördliche Kommunikation - im Allgemeinen wie auch im Hinblick auf Informationssicherheit?
Leadership	Wie stehen die Führungskräfte zu Fragen der Informationssicherheit?
Problemmanagement	Wie geht die Behörde mit Informationssicherheitsproblemen um?
Einstellung	Wie ist die persönliche ?Einstellung gegenüber der Informationssicherheit?
Motivation	Sind die Beschäftigten in Fragen der Informationssicherheit motiviert?
Wahrnehmung	Wie nimmt der/die Einzelne die Informationssicherheit wahr?
Werte	Wie ist das Wertesystem der Mitarbeitenden?
Wissen/Sensibilisierung	Wie sind das Wissen und die Sensibilisierung der Beschäftigten?

Sensipedia
auf der
Lernplattform

Sensipedia

Jeder Besucher soll über das Wiki in die Lage versetzt werden seinen Kenntnisstand entsprechend Informationen und Anleitung...

Status: Offline

Seite | Bearbeiten | Verlauf | Zwischenablage | Was verlinkt hierher? | Druckansicht

Hauptseite

Herzlich Willkommen im Sensipedia. In diesem Wiki erhalten Sie Informationen und Anleitungen rund um die Sensi
Es gibt zwei Möglichkeiten Sensipedia zu verwenden.

1. Wissensabfrage: Suchen Sie dediziert über die "Such"-Funktion nach konkreten Themen
2. Geleitete Tour: Sensipedia leitet sie über Links durch eine Art Tour zu bestimmten Themen (anhand des Leitfadens oder übe

Auf der rechten Seite befindet sich die Wiki-Navigation mit den wichtigsten aktuellen Hauptseiten, um auf ein Thema direkt zuzug
Ein Wiki ist in erster Linie als Nachschlagewerk gedacht, daher bietet es keine Menüstruktur, wie beispielsweise eine Webseite. W
einfach den Zurück-Button Ihres Browsers oder die Wiki-Navigation.

Und jetzt viel Spaß beim Sensibilisieren!

Auf geht´s - Konkrete Aktivitäten direkt anwählen

1. Ich bin zum ersten Mal hier. Was kann ich tun und erfahren?
2. Ich möchte eine Awarenesskampagne durchführen
    1. Ich möchte meine Mitarbeiter sensibilisieren
    2. Ich möchte meine Führungskräfte sensibilisieren
    3. Ich möchte meine IT-Spezialisten sensibilisieren
3. Ich möchte eine Übersicht über vorhandene Materialien
4. Ich möchte nur Schulungen durchführen
    1. Ich möchte nur Mitarbeiter schulen
    2. Ich möchte nur Führungskräfte schulen
5. Ich habe bereits eine Kampagne durchgeführt und möchte weiterführende Maßnahmen ergreifen Was gibt es Neues?
6. Tipps und Tricks

Sensipedia

Jeder Besucher soll über das Wiki in die Lage versetzt werden seinen Kenntnisstand entsprechend Informationen und Anleitung...

Status: Offline

Lernen - Wissen vermitteln

Nachdem Sie das Bewusstsein für Informationssicherheit bei Ihren Kolleginnen und Kollegen „geweckt" haben, sollten Sie Ihre Betroffenheit ist nun der richtige Nährboden für das Erlernen konkreter Verhaltensweisen geschaffen. Geben Sie den Zielgrupp Situationen mit (z. B. was tun, wenn eine vermeintliche infizierte E-Mail ankommt, wie soll sich der Beschäftigte in diesem Fall müssen ein sicheres Passwort verwenden!") sondern bieten Sie eine Lösung an („Ein sicheres Passwort kann folgendermaßen g Es wird eine Wissensbasis benötigt, auf der die Informationen zur Informationssicherheit zusammengetragen und verfügbar ge das Wissen gesucht, verlinkt und multimedial aufbereitet werden kann. Alle Maßnahmen und Informationen sollten hinterlegt w Handlungsempfehlungen, die innerhalb der Initiative angeboten werden.
Für die Lernphase eignen sich natürlich auch typische Schulungen. Dies könnten z. B. sein:

- Präsenzschulungen: Ihre Belegschaft wird gruppenweise in Präsenzterminen geschult. Diese Schulungen können z. B. d „externen" Maßnahme ist die hohe Kompetenz in Sachen Informationssicherheit sowie didaktisches Einfühlungsvermöge Veranstaltungen. Der Lerneffekt durch Präsenzschulungen ist besonders hoch, allerdings ist auf der anderen Seite auch Arbeitsplatz) notwendig.
- Online-Schulungen: Mit einer Online-Schulung können Sie gezielt zu den einzelnen Themengebieten schulen und diese d Mitarbeiterinnen und Mitarbeiter können das Gelernte also direkt in einem Fragenkatalog anwenden. Der Vorteil dieser M Durchführung und einer möglichen (anonymisierten!) Auswertung des Fragenkataloges. Die Durchführung von Online-S gern (bis in die ganz ferne Zukunft) verschoben. Der Lerneffekt gut.
- Workshops mit dem IT-Sicherheitsverantwortlichen: auch der IT-Sicherheitsverantwortliche kann Workshops zum Them Dies kann z. B. auch in Gemeinschaft mit dem Datenschutz- und/oder Geheimschutzbeauftragten durchgeführt werden.

Wir machen weiter

Human Hacking

Bluff-O-Meter – der große Social Engineering Selbsttest

- **Hilfsbereitschaft:**
  zuvorkommend, aufmerksam, dienstbereit.
- **Leichtgläubigkeit:**
  arglos, unkritisch, gutgläubig
- **Neugier:**
  wissbegierig, offen, interessiert
- **(Wunsch nach) Anerkennung:**
  Bestätigung suchend, für Lob empfänglich
- **Druck:**
  leistungsorientiert, hierarchiebewußt, perfektionistisch
- **Angst:**
  vorsichtig, harmoniebewußt, konfliktscheu

Studie: Bluff me if you can, Firma known sense, 2015

Kontakt und Informationen

Lehrgruppe 5 - Dr. Käthe Friedrich

sibe-lg5@bakoev.bund.de

Tel: 0228 99 629 5502

www.bakoev.bund.de/IT-Sicherheitsbeauftragte

www.lernplattform-bakoev.bund.de