SiKoSH
SICHERHEIT FÜR KOMMUNEN
IN SCHLESWIG-HOLSTEIN

Hilfsmittel: Konzept Schulung

Version:	1.0.0
Datum:	16.06.2018
Herausgeber:	Kommunales Forum für Informationstechnik (KomFIT e.V.) Reventlouallee 6 24105 Kiel sikosh@komfit.de https://www.sikosh.de

Inhalt

1 Zielsetzung

Das Schulungskonzept Informationssicherheit regelt die Planung, Vorbereitung, Teilnahmeverpflichtungen und Durchführung von Schulungsveranstaltungen zur Informationssicherheit für Rollenträger innerhalb des Informationssicherheitsmanagementsystems (ISMS).

2 Geltungsbereich

Dieses Konzept gilt für alle Mitarbeiterinnen und Mitarbeiter.

3 Planung

Die Schulungen tragen dazu bei, das in der Informationssicherheitsleitlinie vereinbarte Sicherheitsniveau zu gewährleisten.

3.1 Zielgruppen

Die Inhalte der Schulungsmaßnahmen richten sich an folgende Zielgruppen:

- Führungskräfte
- Assistenzen, Empfänge
- Mitarbeiterinnen und Mitarbeiter ohne Administratorfunktion
- Systemadministratorinnen und Systemadministratoren
- Informationssicherheitsbeauftragte (ISB)

3.1.1 Ziele für die Ebene der Führungskräfte

Die Behördenleitung kann der nicht-delegierbaren Aufgabe der Gesamtverantwortung für die Informationssicherheit nur nachkommen, wenn die Strukturen und Prozesse des ISMS von der anwendenden Behörde bekannt sind.

Ziele: Alle Vorgesetzten

- sind mit den allgemeinen und den speziellen in Ihrem Verantwortungsbereich geltenden Sicherheitsstrukturen und –prozessen vertraut
- kennen die rechtlichen Rahmenbedingungen
- haben die Sicherheitsleitlinie und die Sicherheitskonzeption der Institution verinnerlicht
- und halten die Mitarbeiterinnen und Mitarbeiter zur Einhaltung an, indem sie mit gutem Beispiel vorangehen.

3.1.2 Ziele für Mitarbeiterinnen und Mitarbeiter mit direktem Kundenkontakt (Assistenzen, Empfänge, Kundenbetreuung)

Ziele: Diese Gruppe

- verfügt über Grundwissen der Informationssicherheit
- kann die wesentlichen Sicherheitsregeln für ihren Arbeitsplatz anwenden
- und ist sich der Verantwortung der Einhaltung der Sicherheitsziele im eigenen Zuständigkeitsbereich bewusst.

3.1.3 Ziele für Mitarbeiterinnen / Mitarbeiter ohne Administratorfunktion

Die Mitarbeiterinnen und Mitarbeiter in dieser Gruppe nutzen ihnen bereitgestellte Computerhardware und Verfahren um ihrer Aufgabe der Sachbearbeitung nachkommen zu können ohne eigene

administrative Befugnisse. In dieser Gruppe sind die direkten Berührungspunkte mit IT-Systemen/IT-Anwendungen und der Wissensstand darüber auf Grund der unterschiedlichen Rollen - Softwareentwicklung bis Personalsachbearbeitung - unterschiedlich ausgeprägt.

Ziele: Diese Gruppe

- verfügt über Grundwissen der Informationssicherheit
- kann die wesentlichen Sicherheitsregeln für ihren Arbeitsplatz anwenden
- und ist sich der Verantwortung der Einhaltung der Sicherheitsziele im eigenen Zuständigkeitsbereich bewusst.

Mitarbeiter mit direktem Kundenkontakt, wie zum Beispiel Assistentinnen und Assistenten von Führungspersonen, Mitarbeiterinnen und Mitarbeiter an zentralen oder dezentralen Empfängen und Sachbearbeiterinnen und Sachbearbeiter mit direktem Kontakt zu Kunden sind beliebte Ziele für mehrstufige Angriffe auf die Informationssicherheit. Sie sind zusätzlich zu Phishing-Angriffen (medial vermitteltes Social Engineering) auch direktem Social Engineering ausgesetzt, in vielen Fällten kann ein geschickter Angriff auch direkten Zugriff auf das Arbeitsgerät dieser Mitarbeiterinnen und Mitarbeiter bekommen.

Zusatzziel: Zusätzlich bekommt diese Gruppe eine Einführung in die Techniken und Einsatzfelder des computerbezogenen Social Engineerings.

3.1.4 Ziele für Systemadministratorinnen / Systemadministratoren

Systemadministratorinnen und Systemadministratoren sind für die Herstellung technischer Informationssicherheit verantwortlich. Sie benötigen tiefgehende Fachkenntnisse der von ihnen betreuten IT-Systeme und IT-Anwendungen. Sie sind in der Lage, den Nutzungskontext in der Ausarbeitung technischer Strategien für mehr Informationssicherheit angemessen zu berücksichtigen.

Ziele: Systemadministratorinnen und Systemadministratoren

- sind in der Lage, Sicherheitsprobleme zu erkennen und zu beheben
- sie können Konzepte entwickeln, die Sicherheitsprobleme minimieren
- sie beherrschen die Sicherheitsregularien der anwendenden Institution in ihrem Verantwortungsbereich und können sie anwenden.
- sie sind in der Lage Konflikte zwischen IT-Sicherheit und Datenschutzzielen zu erkennen und können geeignete Strategien zur Auflösung dieser Konflikte entwickeln.

3.1.5 Ziele für Informationssicherheitsbeauftragte (ISB)

ISB sind für alle Belange und Fragen der Informationssicherheit zuständig. Sie arbeiten eng mit den Datenschutzbeauftragten zusammen.

Ziele: ISB

- benötigen ein vertieftes Wissen über die Strukturen und Prozesse eines ISMS und insbesondere der spezifischen Ausprägungen und Regelungen bei der anwendenden Institution

- sie können Konzepte entwickeln, die Sicherheitsprobleme minimieren
- sie kennen die Sicherheitsregularien der anwendenden Institution
- sind in der Lage Bedrohungen der Sicherheitsziele der Behörde zu erkennen und hieraus resultierende Schäden für die eigene Institution bestmöglich zu verhindern.
- sie sind in der Lage Konflikte zwischen IT-Sicherheit und Datenschutzzielen zu erkennen und können geeignete Strategien zur Auflösung dieser Konflikte entwickeln
- haben die für den Aufbau eines ISMS und der Pflege der Sicherheitskonzeption erforderlichen Grundkenntnisse der Methodik des Grundschutzes nach BSI

3.2 Konzept für die Schulung

Grundlage für die Schulungsplanung ist der Baustein ORP.3 (Sensibilisierung und Schulung) des IT-Grundschutzkompendiums.

Das Schulungskonzept folgt den Standards des National Institute of Standards and Technology (NIST)[1], die auch von ENISA[2] und BAköV[3] für die Strukturierung von Sensibilisierungsmaßnahmen übernommen worden sind.

Schulungen im Bereich Informationssicherheit NIST nennt drei unterschiedliche Lernsituationen und Lernkontexte

- Awareness
- Training
- Bildung

Awarenessmaßnahmen sind Maßnahmen zur Steigerung der Aufmerksamkeit für das Thema Informationssicherheit. Informationssicherheit soll den Benutzerinnen und Benutzern als wichtiges Thema bekannt sein und als bedeutsames Thema für den eigenen Arbeits- und Wirkungsbereich anerkannt werden. Beispiele sind Präsentationen zum Datenschutzrecht, Veranstaltungen wie „Die Hacker kommen“, Verteilen von Anleitungen, Rundschreiben des Bürgermeisters, Hinweise auf Berichterstattung in der Presse.

Training will relevante Fähigkeiten und Fertigkeiten vermitteln, richtiges Verhalten stärken, falsche Verhaltensweisen löschen. Training ist für Trainer und Trainierten aufwendiger als Awarenessmaßnahmen und hat starke Übungsanteile.

„**Bildung**“ bezieht sich auf die Ausbildung von Personen, die sich der Informationssicherheit als Profession verschrieben haben. Bildung bezeichnet Spezialisten mit großer Erfahrung und tiefem Verständnis, mit Weitblick und der Fähigkeit schon Anzeichen von Schadsituationen zu erkennen und proaktiv zu reagieren.

SiKoSH geht davon aus, dass für erfolgreiches Lernen von sicheren Verhaltensweisen eine dauerhafte Grundaufmerksamkeit für Angelegenheiten der Informationssicherheit geschaffen und

[1] https://www.nist.gov/
[2] https://www.enisa.europa.eu/
[3] http://www.bakoev.bund.de

aufrechterhalten werden muss. Mit anderen Worten vor der Durchführung von Schulungsmaßnahmen sollten bereits Maßnahmen zur Sensibilisierung gegenüber der Informationssicherheit getroffen werden[4]. SiKoSH empfiehlt die Durchführung von Phishing-Simulationen, da diese in besonderer Weise geeignet sind, die Themen „Datenschutz“ und „Informationssicherheit“ im persönlichen Arbeitskontext der Mitarbeiterinnen und Mitarbeiter und die Organisationskultur einer Einrichtung zu verankern und sichere Verhaltenskomponenten zu trainieren.

Der SiKoSH-Ansatz geht davon aus, dass die Unterstützung der Amtsleitung, eine fehlertolerante Organisationskultur und emotional bereichernde partizipative didaktische Methoden Grundlage für die Nachhaltigkeit von kompetentem Sicherheitshandeln sind.

Da Themen aus dem Bereich Datenschutz und Informationssicherheit in die Berichterstattung der Publikumspresse Eingang gefunden haben, kann eine grundlegende „Awareness“ für den Themenbereich vorausgesetzt werden und für die Sensibilisierungsbemühungen bei den Mitarbeiterinnen und Mitarbeitern kommunaler Einrichtungen genutzt werden. Es ist sinnvoll, die öffentliche Berichterstattung auch in den internen Medien (z.B. Mitarbeiterzeitschrift) aufzugreifen und darzustellen, dass das. was anderen widerfahren ist, auch in der eigenen kommunalen Einrichtung leidvolle Realität werden kann.

Phishing ist der wichtigste Pfad über den Angreifer in kommunale Netzwerke und alle anderen Netzwerke kommen können. In seinen modernen Erscheinungsformen wie „Spear Phishing“ und „Business Email Compromise“ ist ein Phishing-Angriff schwer zu erkennen und Benutzer müssen dauerhaft trainiert werden, um unsichere Verhaltensweisen zu verlernen und sichere Verhaltensweisen zu lernen.

Phishing Simulation ist eine Trainingsmethode mit einem hohen Wirkungsgrad und einem guten Preis-Leistungsverhältnis. Die Methode hat sich in den letzten Jahren als Königsweg für das Training der Mitarbeiterinnen und Mitarbeiter im Umgang mit gefährlichen E-Mails und Websites etabliert. SiKoSH empfiehlt deshalb die regelmäßige Durchführung von Phishing-Trainings in der Form von Phishing-Simulationen, etwa in der Form eines Basistrainings, Trainings zur Festigung sicherer Verhaltensweisen und ad-hoc Trainings beim Auftauchen neuer Phishing-Formen.

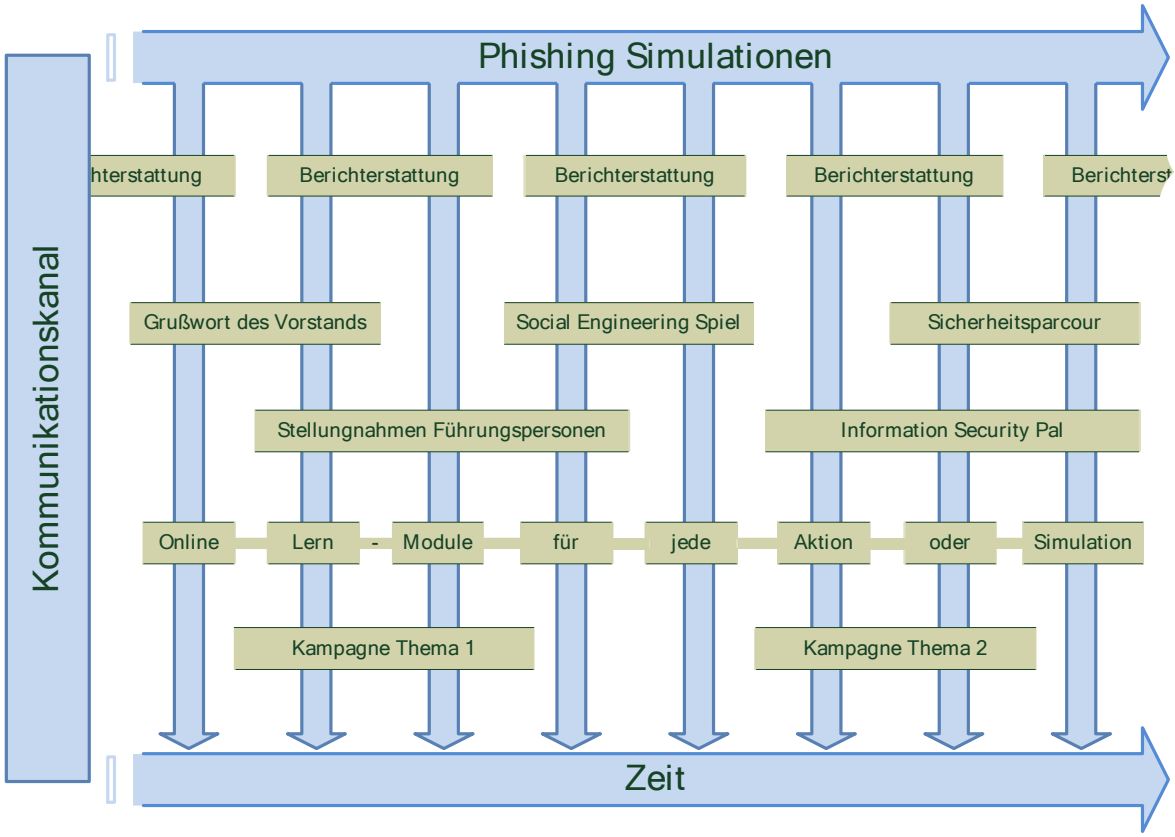
Schulungen zur Verankerung und Vertiefung von sicheren Verhaltensweisen sind effizienter und motivierender, wenn für die Seminargestaltung moderne didaktische Aufbereitungen wie Social Engineering Spiele oder Sicherheitsparcours verwendet werden. Ebenso wichtig ist es Kolleginnen und Kollegen zur Übernahme der (informellen) Rolle des Meinungsführers und Wissensträgers für Fragen der Informationssicherheit zu ermutigen und zu fördern. Probleme der Informationssicherheit treten im Arbeitsfluss unvorhersehbar auf und müssen ad-hoc gelöst werden. Die schnellste und beste Möglichkeit ist „jetzt gleich“ kontextbezogene Hilfe zu bekommen ist immer die Kollegin und der Kollege die sich am besten mit der Lösung eines Problems auskennen und als „information security pal“ die entstandene Verhaltensunsicherheit kompetent und produktiv auflösen können.

[4] S. SiKoSH-Beispiel Sensibilisierung

Es ist in hohem Maße sinnvoll, den erreichten Trainingsstand in einem Online-Schulungssystem[5] abzubilden. Mitarbeiterinnen und Mitarbeiter brauchen die Möglichkeit sich unabhängig von Zeit und Ort zu informieren und das Gelernte zu vertiefen.

Weitere wichtige und aktuelle Themen der Informationssicherheit können und sollen in speziellen Kampagnen thematisiert werden.

Abbildung 1: SiKoSH Schulungskonzept



[5] z. B. https://www.bits-training.de

4 Durchführung von Schulungen

Die Anmeldung zu den Seminaren erfolgt über die jeweiligen Fachvorgesetzten. Die Planung und Durchführung von Schulungsmaßnahme werden vom Informationssicherheitsbeauftragten (ISB) organisiert und dokumentiert. Die Teilnehmerinnen und Teilnehmer erhalten einen entsprechenden Nachweis.

4.1 Ressourcen

Die Schulungen für Mitarbeiter und Mitarbeiterinnen werden in den eigenen Räumen durch den ISB durchgeführt.

Die Qualifikation der Rollenträger im Sicherheitsmanagement selbst wird im Rahmen der Mitwirkung an Arbeitskreisen sowie der Teilnahme an regelmäßigen externen Qualifizierungen durchgeführt.

⇨ Sonstige Festlegungen

- *Schulungskosten*

4.2 Struktur

Die Schulungsmaßnahmen sind modular aufgebaut. Die Schulungsinhalte sind so zusammengefasst, dass jede Zielgruppe entsprechend ihrer betrieblichen Funktion und der benötigten Zielqualifikation hinreichend und in angemessener Tiefe geschult werden kann.

Die Schulungsinhalte sind beschrieben in der Anlage 1.

4.2.1 Spezifische Fachseminare

In Abstimmung mit den jeweiligen Fachbereichen können ergänzende Schulungen, Fach- oder fallspezifische Workshops angeboten werden.

- speziell auf den / die Bedarfsträger zugeschnittener Workshop zur Unterstützung der täglichen Arbeit
- bereichsspezifische oder bereichsübergreifende Fachseminare; diese können technisch oder organisatorisch ausgerichtet sein. Beispielhafte Themen sind:
    - Kryptographie, Protokollierung und Monitoring
    - Firewalls
    - Organisatorische Themen wie Telearbeit, Notfallmanagement und Sicherheitsvorfallmanagement
    - Sicherheitsaspekte bei der Beschaffung
    - Behandlung neuer Technologien im Sicherheitsmanagement
    - Social Engineering
    - Umgang mit Social Media Plattformen.

Die Durchführung erfolgt nach Bedarf. Dauer, didaktische Form und Materialien sind variabel und richten sich an Themenstellung und Teilnehmerkreis aus.

4.3 Methoden und Medien

Die Seminarinhalte werden zielgruppenorientiert in einzelnen Modulen angeboten. Dabei bieten sich Präsenztermine, Onlineseminare und Micro-Teaching (wie z.B. Phishing-Simulationen) als Wissensvermittlungsform an.

4.3.1 Präsenzseminare

Um den Teilnehmern und Lehrkräften ausreichend Möglichkeit zu bieten, fachspezifische Fragen aus ihrem Arbeitsbereich zu erörtern, sollen zu einem Präsenzseminar max. 10-15 Teilnehmerinnen und Teilnehmer eingeladen werden.

Sofern entsprechende Qualifikation und Kapazität zur Verfügung steht, erfolgt die Qualifikation durch das Sicherheitsmanagement. Andernfalls erfolgt die Qualifikation durch externe Anbieter in Absprache mit dem Sicherheitsmanagement und der Leitungsebene.

4.3.2 Online Lernen

Diese Form bietet ein selbstgesteuertes Lernen, d.h. zeit- und ortsunabhängig können verpflichtende Informationen aufgenommen werden. Gerade Dokumente, welche von allen Mitarbeiterinnen und Mitarbeitern zur Kenntnis genommen werden müssen, können hier eingestellt werden. Durch beispielhafte Verständnisfragen, Übungen oder Tests mit vorgegebenen Lösungen wird eine verständige Bearbeitung gefördert.

Technisch kann dokumentiert werden, dass Mitarbeiterinnen bzw. Mitarbeiter ein Dokument aufgerufen haben. So kann das Unternehmen an dieser Stelle nachweisen, dass es den gesetzlichen Vorgaben entsprechend, die Mitarbeiterinnen und Mitarbeiter unterwiesen hat.

4.3.3 Microteaching

Handeln kann man nur durch Handeln erlernen. Damit neue, bisher nicht gezeigte Handlungsweisen in das Verhaltensrepertoire übernommen werden können, müssen sie vorher unter erleichternden Bedingungen kennengelernt und trainiert werden.

Unter Micro-Teaching versteht man den Versuch, komplexe Verhaltenssituationen in „verkleinerten“ Bedingungen zu lernen und zu üben, d.h. kurze Zeitdauer, wenige Teilnehmende, überschaubarer Stoff.

Ziel des Micro-Teaching ist es durch ein Verhaltenstraining den Transfer des Verhaltens in die Praxis vorzubereiten, in der Regel nach dem Muster

- Vermittlung theoretischen Hintergrundwissens;
- Methoden zur kognitiven Aneignung spezifischen Verhaltens und
- praktische Übungen im Anwendungskontext mit
- Feedback.

Verhaltenswirksam sind dabei vor allem die Komponenten „praktische Übungen im Anwendungskontext“ und „Feedback“.

5 Schlussbestimmung / Inkrafttreten

Diese Richtlinie tritt mit dem Tag der Veröffentlichung in Kraft

6 Änderungsverzeichnis

Version	Datum	Kapitel, Änderung	Autor/in

Anlage 1: Schulungsinhalte

6.1.1 Modul 1: Allgemeine Grundlagen der Informationssicherheit

Dauer:	[ca. 2 Stunden]
Inhalte:	• Motivation und Prinzipien der Informationssicherheit • Gesetze und Verordnungen • Informationssicherheit am Arbeitsplatz • Abschließen der Büroräume • Verwendung sicherer Passwörter • Schutz von Dateien (Lese-/Schreibschutz, Archivierung) • sicherheitsbewusstes Verhalten am Arbeitsplatz • Wesentliche Sicherheitsregeln bei der anwendenden Institution •
Intervall:	Bei Eintritt, [Auffrischung alle 3 Jahre]
Referent(in):	[ISB]
Adressaten:	Alle Mitarbeiterinnen und Mitarbeiter
Schulungsform:	[Inhouse-Seminar]

6.1.2 Modul 2: Informationssicherheit und Regularien (Führungskräfte, Fachverantwortliche)

Dauer:	ca.2 Stunden
Inhalte:	• Sicherheitsrichtlinie und Sicherheitskonzeption/Sicherheitskonzept • Informationssicherheitsstrukturen bei der anwendenden Institution • Philosophie und Ziele von IT-Grundschutz • IT-Grundschutzmethodik • Umgang mit den Grundschutzkatalogen • BSI-Standards und Verwendung bei der anwendenden Institution • Sensibilisierung der Führungskräfte für die Informationssicherheit • Einsatz von „internen Kontrollsystemen“ (IKS) • Notfallvorsorgemanagement • Verhalten im Notfall und bei Informationssicherheitsvorfällen • ausgewählte technische, infrastrukturelle und organisatorische Maßnahmen zur Sicherstellung von Informationssicherheit.
Referent(in)	[ISB]
Intervall:	Bei Eintritt, [Auffrischung alle 3 Jahre]
Adressaten:	Führungskräfte
Schulungsform:	[Inhouse-Seminar]

6.1.3 Modul 3: Rollenträger im Sicherheitsmanagement

Dauer:	5 Tage
Inhalt:	• Informationssicherheit - Anforderungen und aktuelle Entwicklungen • rechtliche und organisatorische Rahmenbedingungen für Informationssicherheit • Datenschutz und Informationssicherheit • Standards und Zertifizierung • Sicherheitsmanagement und Informationssicherheitsleitlinie • Informationssicherheit nach IT-Grundschutz • Sensibilisierungs- und Schulungskonzept • Meldewege, Behandlung von Sicherheitsvorfällen und Notfallvorsorge • Reifegradmessung, Aufrechterhaltung der Informationssicherheit und Revision • IT-Sicherheitsbeauftragte im Sicherheitsmanagement - Kommunikation und Kooperation • Aktuelle Entwicklungen in der Modernisierung des IT-Grundschutzes und deren Anwendung • Berichterstattung und Präsentation von Arbeitsergebnissen
Intervall:	Bei Rollenübernahme sowie bedarfsorientierte Auffrischung
Referent(in):	BAKOEV oder vergleichbar
Adressaten:	Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, IT-Verantwortliche
Schulungsform:	Seminar z. B. Lehrgang IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I - Basis Kompakt der BAKOEV

6.1.4 Modul 4: Sensibilisierungsmaßnahmen

Dauer:	Ca. 5 Stunden

Inhalt:	• Grundlagen (Informationssicherheit und Datenschutz)
	• Allgemeine Maßnahmen
	• Spezifische Bedrohungen und Maßnahmen
	  o Mobile Geräte (Smartphones, Notebooks, Datenträger)
	  o Internet-Dienste (www, E-Mail, Social Media, Cloud)

Intervall:	Bei Eintritt und [regelmäßig alle 3 Jahre]
Referent(in):	ISB, [DSB und ggf., weitere (z. B. Leiter Gebäudemanagement)]
Adressaten:	Alle Mitarbeiterinnen und Mitarbeiter
Schulungsform:	[Die Schulungsformen ergeben sich aus dem Sensibilisierungskonzept.] • Vorbereitende Maßnahmen zur Bewusstseinsschärfung (Phishing-Kampagne). • Online-Training BITS • Intranet, Mitarbeiterzeitung • Inhouse-Seminare