Der neue Leitfaden für die Praxis:

Wege zu mehr Bewusstsein für Informationssicherheit

Juli 08

enisa
European Network and Information Security Agency

Die ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine Einrichtung der Europäischen Union, die mit dem Ziel errichtet wurde, die Funktionsfähigkeit des Binnenmarktes zu fördern. Als Kompetenzzentrum berät die ENISA die Mitgliedstaaten und die Einrichtungen der Europäischen Union über Netzwerk- und Informationssicherheit, spricht Empfehlungen aus und dient als zentrale Anlaufstelle für Informationen über bewährte Praktiken. Darüber hinaus erleichtert diese Einrichtung die Kontaktaufnahme zwischen den europäischen Institutionen, den Mitgliedstaaten und den privaten Akteuren aus Wirtschaft und Industrie.

Kontakt

Allgemeine Anfragen zu Sensibilisierungsmaßnahmen zur Informationssicherheit richten Sie bitte an:

Isabella Santa, Senior Expert Awareness Raising – E-Mail: awareness@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Der neue Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit

Juli 2008

Inhalt

Zusammenfassung

Zwei Jahre nach der Veröffentlichung der ersten Ausgabe des *Leitfadens für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit* hat die ENISA eine Neubearbeitung dieses Leitfadens vorgenommen und den Inhalt um neue Erkenntnisse aus Forschung und Analyse ergänzt. Die neue Ausgabe enthält ein neues Prozessmodell sowie die Beschreibung neuer Maßnahmen und Aufgaben, ergänzt durch Schlüsselleistungsindikatoren und Fallbeispiele.

In den zurückliegenden Jahren sind bei zahlreiche hilfreiche Vorschläge von Nutzern eingegangen, die mit dem Leitfaden arbeiten, die wir zum Teil in der neuen Ausgabe aufgreifen. Bei der Neugestaltung mussten zwar auch Hindernisse überwunden werden, doch ist es uns gelungen vier wesentliche Verbesserungen einzuführen. Neben statistischen Angaben aus Forschungsarbeiten wurden ausführlichere Beschreibungen von Maßnahmen aufgenommen, außerdem wurden Prozessabläufe dargestellt und das Layout wurde überarbeitet, sodass die Leser den Leitfaden jetzt flexibler nutzen können.

Von den vier angesprochenen Verbesserungen fällt die neue Prozesserfassung am ehesten ins Auge. In diesem Zusammenhang werden die wichtigsten Prozesse beschrieben, die notwendig sind, um Initiativen zur Sensibilisierung für Informationssicherheit zu planen, zu organisieren und durchzuführen: Planung, Beurteilung und Konzeption, Ausführung und Abwicklung sowie Evaluierung und Optimierung. Jeder einzelne Prozess wird analysiert und die jeweiligen zeitbezogenen Aktivitäten und zeitlichen Abhängigkeiten bestimmt. Das vorgestellte Prozessmodell dient als Basis für die Aufnahme der Abgrenzungs- und Planungsaktivitäten sowie für die Ausführung und Evaluierung eines Programms. Ziel des Leitfadens ist es, den Lesern eine konsistente, belastbare Sichtweise der wichtigsten Prozesse, Aktivitäten und Aufgaben zu vermitteln.

Die Planungs- und Beurteilungsphase wird als entscheidend für den Erfolg eines Programms angesehen. Im vorliegenden Leitfaden wird insbesondere auf die Bedeutung der folgenden Aspekte eingegangen: Festlegung der Ziele und Zielvorgaben für Sensibilisierungsprogramme, Bestimmung der Zielgruppen, Ausarbeitung eines Kommunikationsplans und Messung des Erfolgs von Sensibilisierungsprogrammen. Darüber hinaus wird darauf hingewiesen, wie wichtig ein Veränderungsmanagement-Konzept für Sensibilisierungsinitiativen ist, denn ein solches Konzept hilft, die Kluft zwischen einem bestimmten Problemfeld und den menschlichen Reaktionen auf die erforderlichen Veränderungen zu überbrücken.

Die zweite und für viele Nutzer vermutlich wichtigste und hilfreichste Verbesserung in der neuen Ausgabe betrifft die Festlegung von Schlüsselleistungsindikatoren, die Organisationen ermöglichen, die Effektivität von Sensibilisierungsprogrammen zu beurteilen. Diese Indikatoren wurden den wichtigsten Prozessen und Organisationsebenen zugeordnet. Diese Daten in einer für die Ausarbeitung von Sensibilisierungsprogrammen optimalen Weise zusammenzuführen, war nicht einfach.

Die dritte wichtige Verbesserung betrifft die Aufnahme von Fallbeispielen und Erfahrungen zu verschiedenen Sensibilisierungsaspekten aus unterschiedlichen Organisationen. Sie helfen den Lesern dabei, zentrale Problemstellungen, Schwierigkeiten, Lösungsmöglichkeiten usw. zu erkennen, und tragen so dazu bei, dass die Vorschläge für Maßnahmen und Empfehlungen noch besser verständlich und damit wirkungsvoller sind. Auf diese Weise werden die Leser unmittelbar angesprochen und die Lernerfahrung vertieft.

Die vierte wichtige Verbesserung ist die Aufnahme weiterer Vorlagen und Muster für das empfohlene Instrumentarium. Dadurch wird den Lesern die Vorbereitung und Durchführung von Sensibilisierungsprogrammen erleichtert. Die Anhänge enthalten unter anderem eine Vorlage für ein

Formular zur Erfassung gewonnener Erfahrungen, ein Arbeitsblatt zur Ermittlung der Ausgangsbasis für eine Initiative zur Sensibilisierung für Informationssicherheit, einen Fragebogen zur Sensibilisierung sowie eine Vorlage für die Erfassung von Zielgruppendaten.

Daneben wird in dem Leitfaden aber auch auf Erfolgshindernisse hingewiesen und er bietet praxisbezogene Ratschläge, wie derartige Hindernisse in der Planungs- und Durchführungsphase von Programmen aus dem Weg geräumt werden können. Außerdem werden die wesentlichen Faktoren aufgezeigt, die über den Erfolg einer Initiative zur Informationssicherheit entscheiden.

Die ENISA hofft, den Lesern mit diesem neuen Leitfaden ein wertvolles Hilfsmittel für die Vorbereitung und Durchführung von Sensibilisierungsprogrammen in Unternehmen und öffentlichen Einrichtungen an die Hand zu geben. Informationssicherheit zu schaffen, ist eine enorme Aufgabe – spezifische Zielgruppen für das Thema zu sensibilisieren, ein wichtiger erster Schritt zur Bewältigung dieser Aufgabe.

TEIL 1: DIE BEDEUTUNG VON PROGRAMMEN ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT

Einführung

Wir leben in einem digitalen Zeitalter – für Bürger und Unternehmen gleichermaßen sind die Informations- und Kommunikationstechnologien (IKT) bei ihrer täglichen Arbeit zu einem unverzichtbaren Hilfsmittel geworden. Zugleich sind Bürger wie Unternehmen aber zunehmend durch Angriffe gegen die Informationssicherheit gefährdet. Grund hierfür ist die Anfälligkeit der neuen und auch der bereits seit längerem genutzten Technologien und – parallel hierzu – die vermehrte Nutzung von ständig aktivierten Online-Verbindungen sowie das Hinzukommen neuer Nutzer in den Mitgliedstaaten, deren Zahl exponential ansteigt. Sicherheitsverstöße können durch die Anwendung von Informationstechnologien verursacht werden, beispielsweise durch Computerviren oder andere Schadprogramme, Systemausfälle oder Datenverfälschungen, oder aber sie haben soziale Hintergründe, wie etwa der Diebstahl von Bürogeräten. In einem Zeitalter, das in wachsendem Maße auf digital aufbereitete Informationen angewiesen ist, wächst auch die Zahl der Gefahren. Nicht wenige Bürger sind sich ihrer Gefährdung durch Sicherheitsrisiken in diesem Bereich nicht bewusst, wie Vorfälle aus jüngster Zeit bestätigen.

So wurde einem Mitarbeiter der Finanzbehörde im Vereinigten Königreich ein Laptop mit Daten von rund 2 000 Bürgern mit steuerbegünstigten Sparkonten, sogenannten ISA-Konten, gestohlen; dem britischen Finanzamt kamen die personenbezogenen Daten von 6 500 Beziehern von privaten Altersvorsorgeleistungen abhanden; bei neun Versorgungswerken des britischen staatlichen Gesundheitsdienstes NHS gingen auf CD gespeicherte Patientenakten verloren.([1]) Den schwedischen Streitkräften wurde ein an einem öffentlich zugänglichen Rechner zurückgelassener USB-Speicherstick ausgehändigt, der neben nicht vertraulichen Daten auch geheime Informationen zur Bedrohungslage durch unkonventionelle Spreng- und Brandvorrichtungen und Minen in Afghanistan enthielt;([2]) USB-Speichersticks mit geheimen Militärinformationen der US-Armee wurden auf einem Basar bei Bagram (Afghanistan) zum Kauf angeboten.([3]) In den USA kamen die Daten von drei Millionen britischen Fahrschülern abhanden,([4]) und in einer Mailsendung des California Public Employees' Retirement System (kalifornischer Rentenfonds für Angestellte im öffentlichen Dienst) wurden die Sozialversicherungsnummern der Mitglieder offengelegt. Diese Beispiele unterstreichen, wie wichtig es ist, dass Geschäfts- und Kundendaten geschützt werden, ganz gleich, ob sie in Datenzentren, Netzwerken oder in Ausdrucken

([1]) ENISA, *Sicherer Umgang mit USB-Speichersticks,* 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_de.pdf
([2]) Jevans, Dave, *Privacy and identity theft,* IronKey, im Internet abrufbar unter http://blog.ironkey.com/?cat=9&paged=2 (zuletzt aufgerufen am 20. Mai 2008).
([3]) Watson, Paul, „US military secrets for sale at Afghanistan bazaar", *Los Angeles Times*, 10. April 2006.
([4]) Ford, Richard, „Disc listing foreign criminals lost for year" *The Times,* 20. Februar 2008, im Internet abrufbar unter http://www.timesonline.co.uk/tol/news/politics/article3399712.ece (zuletzt aufgerufen am 15. Juli 2008).

und Postsendungen abgelegt sind.([5])

Angesichts der Zunahme und immer weiteren Ausbreitung von Sicherheitsverstößen sind die Lösungen, die heute für Informationssicherheit sorgen, morgen bereits überholt. Während die Sicherheitslandschaft ständigen Veränderungen unterworfen ist, gehen die meisten Analytiker davon aus, dass der Faktor Mensch im Gesamtrahmen der Informationssicherheit das schwächste Glied ist. Wenn dem so ist, kann die Zahl der Verstöße gegen die Informationssicherheit nur durch einen tiefgreifenden Wandel in der Wahrnehmung der Nutzer oder in der Organisationskultur effektiv verringert werden.

Aufgabenstellung

Bei der ENISA ist man sich der Tatsache bewusst, dass die Sensibilisierung für mögliche Risiken und die vorhandenen Sicherheitsmaßnahmen zu deren Abwehr den ersten Schritt zur größeren Sicherheit von Informationssystemen und -netzen darstellt.([6]) Mit diesem Leitfaden sollen daher öffentlichen und privaten Organisationen – also Behörden, öffentlichen Einrichtungen und Unternehmen – praxisbezogene Ratschläge für die Vorbereitung und Durchführung von Initiativen zur Sensibilisierung für Informationssicherheit([7]) an die Hand gegeben werden.

Hierzu enthält der Leitfaden eine ausführliche Anleitung, die als Ausgangsbasis für die Konzeption, Entwicklung und Umsetzung wirksamer und zielgerichteter Sensibilisierungsprogramme bis hin zur Evaluierung des Programms herangezogen werden kann. Es wird aufgezeigt, wie der Sensibilisierungsbedarf ermittelt, ein Plan entwickelt und die Finanzierung von Sensibilisierungsinitiativen durch die Organisation sichergestellt werden können. Außerdem werden folgende Bereiche beschrieben:

- ✓ Auswahl von Sensibilisierungsthemen
- ✓ Entwicklung eines Geschäftsszenarios
- ✓ Schaffung eines Kommunikationsrahmens
- ✓ Nutzung verschiedener Kanäle für die Durchführung der Sensibilisierungsinitiative
- ✓ Evaluierung der Wirksamkeit des Programms
- ✓ Aktualisierung und Verbesserung des Programms

Dieser neue Leitfaden basiert neben Untersuchungen und Analysen der ENISA auf öffentlich zugänglichen Informationen, die der ENISA von Organisationen und Mitgliedern der ENISA-Plattform für die Zusammenarbeit bei der Sensibilisierung([8]) zur Verfügung gestellt wurden.

([5]) ENISA, *Sicheres Drucken,* 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing_de.pdf; Basiliere, Pete, *Information breach highlights production print and mail vulnerabilities,* Gartner, 18. September 2007.

([6]) OECD, *Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security (Umsetzungsplan für die OECD-Richtlinien für die Sicherheit von Informationssystemen und -netzen: Auf dem Weg zu einer Sicherheitskultur),* DSTI/ICCP/REG(2003)5/REV1, Working Party on Information Security and Privacy (Arbeitsgruppe für Informationssicherheit und Privatsphäre), OECD, 2003, im Internet abrufbar unter http://www.oecd.org/dataoecd/23/11/31670189.pdf; Herold, Rebecca, *Addressing the insider threat,* IT Compliance in Realtime, Realtime publishers, Mai 2008, Volume I, Number 3, im Internet abrufbar unter http://nexus.realtimepublishers.com/RTITC.htm (zuletzt aufgerufen am 31. Juli 2008).

([7]) Im vorliegenden Leitfaden werden die Begriffe Sensibilisierungsinitiative und Sensibilisierungsprogramm gleichbedeutend verwendet.

([8]) Die Plattform für die Zusammenarbeit bei der Sensibilisierung (Awareness Raising Community) ist eine offene, gebührenfreie Plattform für alle Experten, die ein Interesse daran haben, die Sensibilisierung für die Informationssicherheit in ihren Organisationen zu verbessern. Die Plattform für die Zusammenarbeit bei der Sensibilisierung wurde im Februar 2008 eingerichtet, um gemeinsam mit der Projektgruppe Sensibilisierung der

Ziele

Nachstehend werden die Ziele genannt, die die ENISA mit diesem Leitfaden verfolgt:

- ✓ Anhand einer beispielhaften Strategie soll dargestellt werden, wie Maßnahmen zur Sensibilisierung und Schulung für Informationssicherheit durchgeführt werden können.
- ✓ Risiken, die im Zusammenhang mit Sensibilisierungsinitiativen auftreten, werden herausgearbeitet, damit sie bei künftigen Maßnahmen vermieden werden können.
- ✓ Es wird ein Bezugsrahmen vorgegeben, anhand dessen eine Evaluierung der Wirksamkeit von Sensibilisierungsprogrammen vorgenommen werden kann.
- ✓ Es wird ein Kommunikationsrahmen vorgeschlagen.
- ✓ Die vorgestellten Vorlagen und Hilfsmittel können den mit der Durchführung von Sensibilisierungskampagnen betrauten Teams als Grundlage dienen.
- ✓ Mit dem Leitfaden soll ein Beitrag zum Entstehen einer Kultur der Informationssicherheit in den Mitgliedstaaten geleistet werden, indem die Nutzer dazu angehalten werden, verantwortungsbewusst zu handeln und verstärkt auf Sicherheit zu achten.

Zielgruppen

Der vorliegende Leitfaden richtet sich an spezielle Schlüsselzielgruppen in öffentlichen oder privaten Organisationen, wie Leiter der Informationstechnologie (Chief Information Officer, CIO), IT-Sicherheitsbeauftragte und -Mitarbeiter, Führungskräfte der mittleren Führungsebene einschließlich Mitarbeiter und Auftragnehmer sowie Mitarbeiter im Personalwesen.

Sensibilisierung – Definition

Sensibilisierung ist der Zweck der Aufklärungsstrategie einer Organisation, mit der versucht werden soll, die Verhaltensweisen der jeweiligen Zielgruppe (z. B. Mitarbeiter, Öffentlichkeit usw.) zu verändern; Sensibilisierung ist nicht mit einer Schulung gleichzusetzen. Sensibilisierungsmaßnahmen werden deshalb kontinuierlich und auf verschiedenen Wegen durchgeführt, sie sind zudem weniger formal und kürzer als Schulungsmaßnahmen.

In der NIST-Sonderveröffentlichung 800-16 wird Sensibilisierung folgendermaßen definiert: „Sensibilisierung ist nicht mit einer Schulung gleichzusetzen. Der Zweck von Veranstaltungen zur Sensibilisierung besteht darin, die Sicherheit in den Blickpunkt zu rücken. Veranstaltungen zur Sensibilisierung sollen die Zielgruppe in die Lage versetzen, Zwischenfälle im Bereich der Informationssicherheit zu erkennen und angemessen zu reagieren. Bei Sensibilisierungsmaßnahmen ist der Lernende der Empfänger von Informationen, während er bei einer Schulung eine aktivere Rolle spielt. Bei der Sensibilisierung kommt es darauf an, mit attraktiven Informationsangeboten ein möglichst breites Spektrum an Zielgruppen zu erreichen. Eine Schulung hat einen formaleren Rahmen und ist darauf ausgerichtet, Wissen und Kenntnisse zu vermitteln, die die Arbeitsleistung verbessern."([9])

Schulung zählt zu den Instrumenten, mit denen Sicherheitsmaßnahmen umgesetzt werden. Ein Schulungsprogramm sollte entsprechend den von der Organisation vorgegebenen Lernzielen gestaltet und durchgeführt werden. Folglich werden in einer Schulung Kenntnisse vermittelt, die dem

---

ENISA eine Kultur der Informationssicherheit zu fördern und die Abteilung bei ihrer Arbeit zu unterstützen. Siehe ENISA, *Key facts and figures about the AR Community and its members*, 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/ar_comm_key_facts.pdf

([9]) NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, im Internet abrufbar unter http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (zuletzt aufgerufen am 21. Juli 2008).

Teilnehmer die Ausübung einer bestimmten Funktion ermöglichen, während das Ziel einer Sensibilisierungsmaßnahme darin besteht, die Aufmerksamkeit des Teilnehmers auf ein bestimmtes Thema oder einen Themenbereich zu lenken. Die in einer Schulung vermittelten Kenntnisse bauen auf dem Fundament der Sensibilisierung auf, insbesondere dem Material, das zur Vermittlung von Basiswissen und Kompetenzen im Bereich der Informationssicherheit verwendet wurde.([10])

Sensibilisierungsprogramme beginnen mit der Sensibilisierung, nehmen ihren weiteren Verlauf über Schulungsmaßnahmen und münden schließlich in die Aufklärung der Zielgruppe. Sie sollten auf die spezifische Zielgruppe zugeschnitten sein, an die sie sich richten. Deshalb ist es sehr wichtig zu bestimmen, welche Nutzer an den beiden Programmformen teilnehmen. Zur Bestimmung der Zielgruppen können verschiedene Methoden eingesetzt werden. Die ENISA hat ein einfaches Instrument entwickelt, mit dem Zielgruppen besser ermittelt und die entsprechenden Daten erfasst werden können. Näheres dazu erfahren Sie im Abschnitt „Zielgruppen bestimmen".([11])

Wann sind Programme zur Informationssicherheit notwendig?

Es sind unterschiedliche Ereignisse und Situationen, die – private oder öffentliche – Organisationen dazu veranlassen, Maßnahmen zur Sensibilisierung für Informationssicherheit durchzuführen. Meist handelt es sich um interne oder externe Faktoren, die die Organisation selbst betreffen.

Daher wird unterschieden zwischen reaktiven Maßnahmen, die zum Beispiel nach einem Datenverlust ergriffen werden, und Initiativen, die im Rahmen einer allgemeinen Informationssicherheitspolitik oder -strategie geplant werden. Nachfolgend sind einige der wichtigsten Ereignisse und Situationen aufgeführt, die ein Programm zur Sensibilisierung für Informationssicherheit erfordern können.

Externe Faktoren

- ✓ Neue gesetzliche Regelungen
- ✓ Regierungswechsel
- ✓ Informationstag oder -woche zum Thema Sensibilisierung auf nationaler Ebene
- ✓ Neues nationales, regionales oder lokales Programm zu Grundlagen der Informationssicherheit für die Bürger
- ✓ usw.
- ✓

Interne Faktoren

- ✓ Neue gesetzliche Regelungen und Vorschriften, die für die Organisation relevant sind
- ✓ Neue Sicherheitspolitik und/oder -strategie
- ✓ Aktualisierungen oder Änderungen der Strategien, Verfahren, Standards und Leitlinien zur Informationssicherheit
- ✓ Einführung einer neuen Technologie

([10]) NIST, *Information technology security training requirements: A role- and performance-based model,* NIST — SP 800-16, USA, 1998, im Internet abrufbar unter http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (zuletzt aufgerufen am 21. Juli 2008).
([11]) Herold, Rebecca, *Information security and privacy awareness program,* Auerbach Publications, USA, 2005; NIST, *Building an information technology security awareness program*, NIST — SP 800-50, NIST, 2003, im Internet abrufbar unter http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (zuletzt aufgerufen am 17. Juli 2008).

- ✓ Neue Mitarbeiter, Auftragnehmer oder Mitarbeiter von Fremdfirmen, die in der Organisation eingesetzt werden
- ✓ Neue Unternehmensleitung
- ✓ Verstärkte Automatisierung
- ✓ Schulung zu den Grundlagen der Informationssicherheit für das gesamte Personal
- ✓ Produktpalette
- ✓ Markteinführung neuer Produkte und Dienstleistungen
- ✓ Einführung neuer Systeme
- ✓ Übernahmen, Fusionen und Veräußerungen
- ✓ Aktuelle Sicherheitsverstöße, -bedrohungen und -vorfälle
- ✓ Neue Risiken
- ✓ Zertifizierung
- ✓ usw.

TEIL 2: DIE WICHTIGSTEN PROZESSE FÜR DIE DURCHFÜHRUNG VON PROGRAMMEN ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT

Allgemeine Strategie für die Durchführung von Programmen zur Sensibilisierung für Informationssicherheit

Die ENISA hat drei Prozesse ermittelt, die bei der Entwicklung eines Programms zur Sensibilisierung für Informationssicherheit besonders wichtig sind: Planung, Beurteilung und Konzeption; Ausführung und Abwicklung sowie Evaluierung und Optimierung.([12])

Prozess	Beschreibung
Planung, Beurteilung und Konzeption	Bei der Konzeption von Sensibilisierungsprogrammen müssen die Aufgaben einer Organisation berücksichtigt werden. Es ist wichtig, dass sie auf die betrieblichen Erfordernisse der Organisation eingehen und für die Kultur sowie gegebenenfalls auch die IT-Architektur der Organisation relevant sind. Am erfolgreichsten sind Programme, die von den Nutzern als relevant für die Thematik und die genannten Belange angesehen werden. In der Konzeptionsphase des Programms werden der Sensibilisierungsbedarf ermittelt, ein wirksamer Plan für die Sensibilisierung entwickelt, die Zustimmung der Führungsebene gesucht und sichergestellt sowie die Prioritäten festgelegt.
Ausführung und Abwicklung	Dieser Prozess schließt alle Aktivitäten ein, die zur Durchführung eines Sensibilisierungsprogramms notwendig sind. Die Initiative kann nur ausgeführt und abgewickelt werden, wenn ✓ eine Bedarfsanalyse durchgeführt wurde; ✓ eine Strategie entwickelt wurde; ✓ eine Plan für das Sensibilisierungsprogramm zur Umsetzung dieser Strategie erstellt wurde; ✓ Material erarbeitet wurde.
Evaluierung und Optimierung	Formale Evaluierungs- und Feedback-Mechanismen sind wichtige Elemente jedes Sensibilisierungsprogramms. Eine kontinuierliche Verbesserung ist nur möglich, wenn klar ist, wie das bestehende Programm funktioniert. Außerdem muss der Feedback-Mechanismus so gestaltet sein, dass die ursprünglichen Ziele des Programms berücksichtigt werden. Sobald die grundlegenden Anforderungen festgelegt sind, kann eine Feedback-Strategie entwickelt und umgesetzt werden.

In diesem Kapitel werden die einzelnen Schritte in der Entwicklung, Ausführung und Evaluierung eines Programms beschrieben, um zeitbezogene Aktivitäten und zeitliche Abhängigkeiten zu ermitteln.

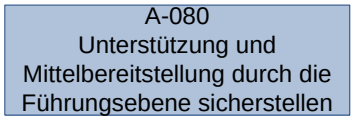
Das auf diese Weise erarbeitete Prozessmodell dient als Basis für die Aufnahme der Abgrenzungs- und Planungsaktivitäten sowie für die Ausführung und Evaluierung eines Programms und vermittelt eine einheitliche, tragfähige Sichtweise der wichtigsten Prozesse, Aktivitäten und Aufgaben. Die vollständige Prozesserfassung ist im Anhang aufgeführt.

([12]) Wilson, Mark, und Hash, John, *Building an information technology security awareness program*, NIST, USA, 2003, im Internet abrufbar unter http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (zuletzt aufgerufen am 17. Juli 2008).

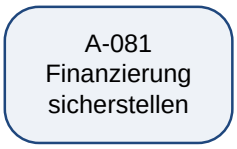
Hierarchie der Prozesserfassung

Die Prozesserfassung folgt einer bestimmten Hierarchie, an deren Beginn die Prozesse stehen und die mit den geschäftsbezogenen Tätigkeiten endet.

Prozess: Darstellung zeitbezogener Aktivitäten und zeitlicher Abhängigkeiten, mit denen durch bestimmte Maßnahmen bestimmte Ergebnisse erreicht werden (zum Beispiel Planung, Beurteilung und Konzeption).



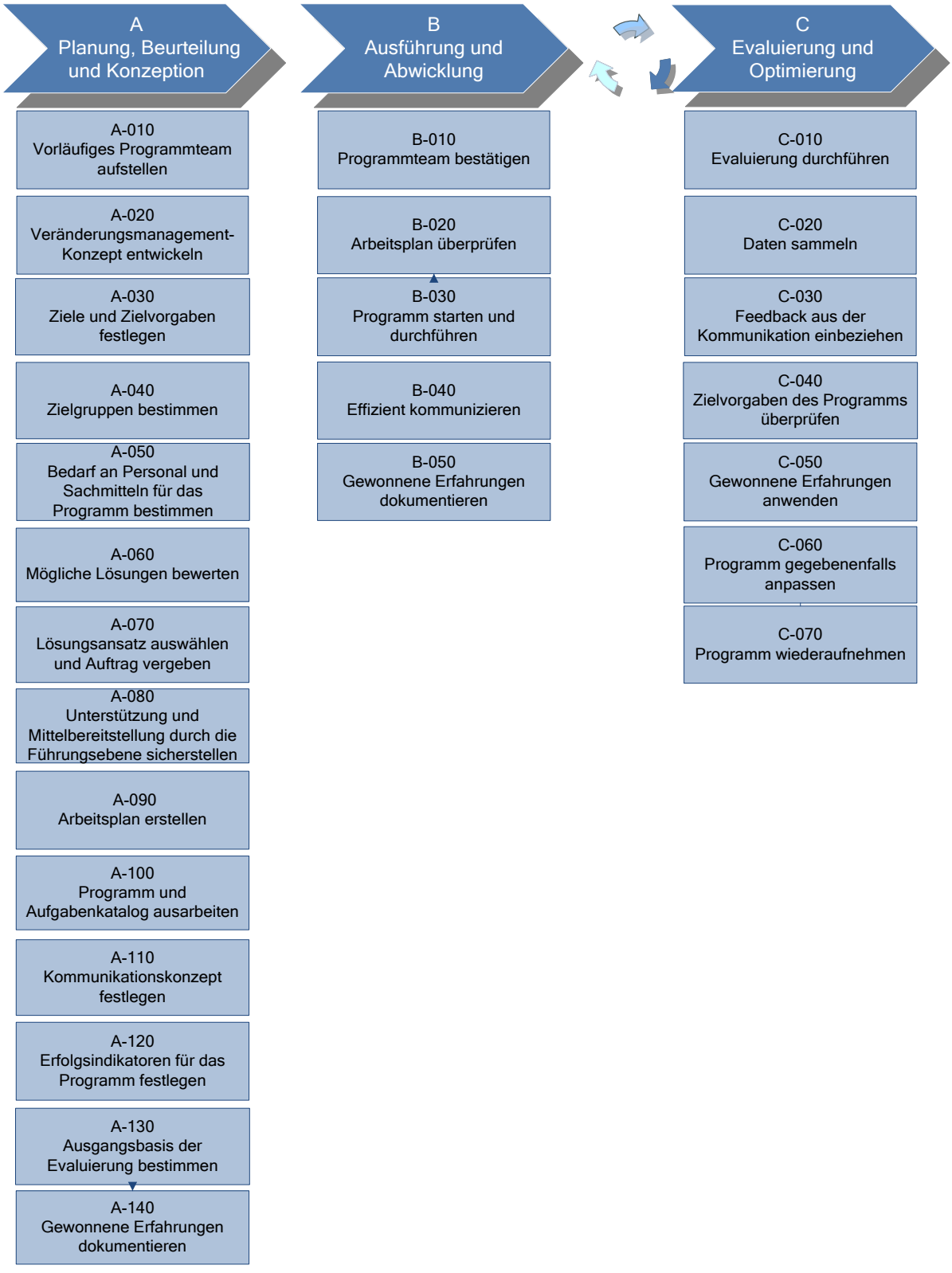
Teilprozess: Teil eines Kernprozesses, der einen bestimmten Tätigkeitsbereich betrifft (beispielsweise die erforderliche Unterstützung und Mittelbereitstellung durch die Führungsebene sicherstellen).



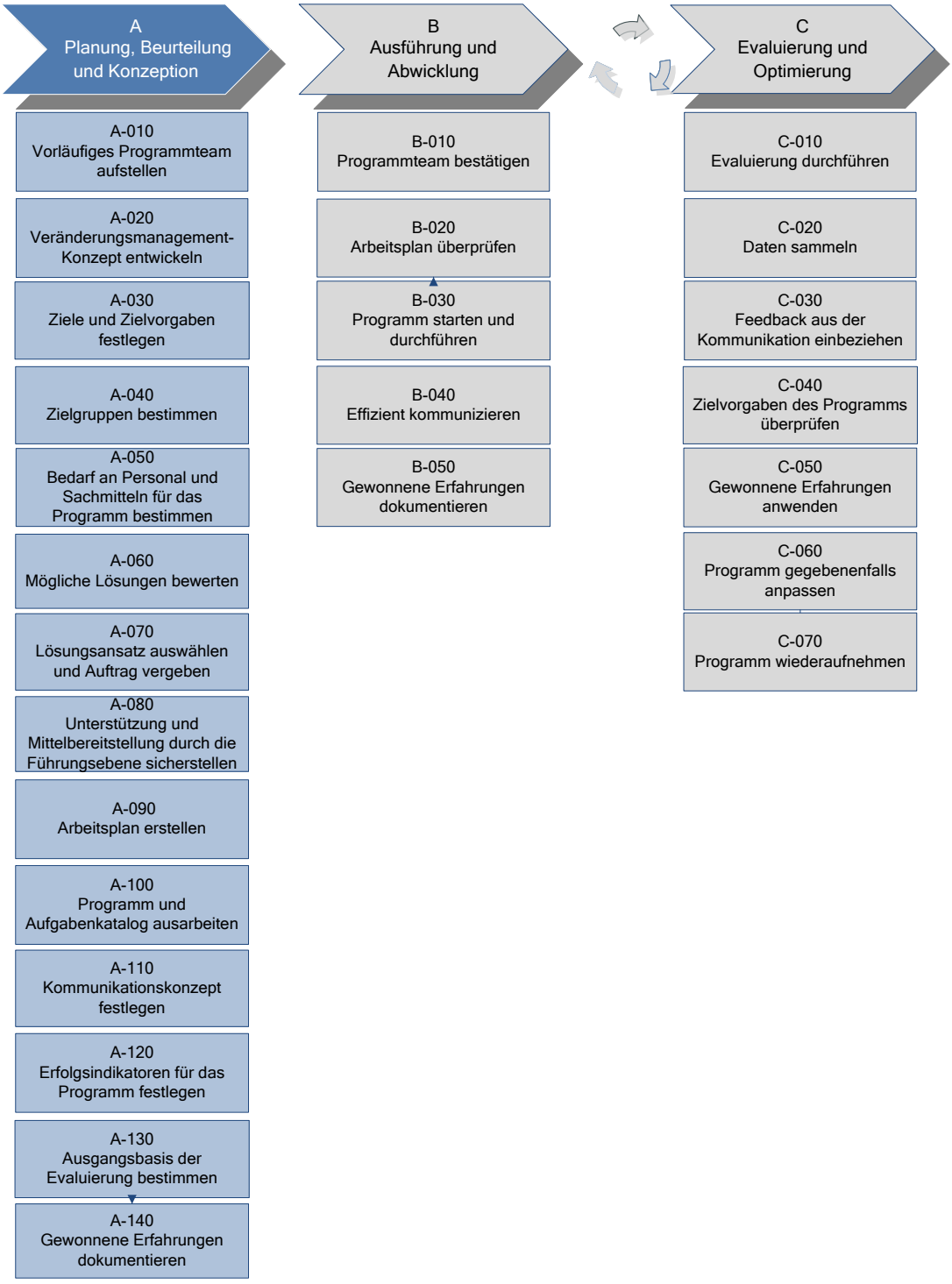
Tätigkeit: Komponente eines Teilprozesses, die ein messbares Ergebnis erbringt (beispielsweise die Finanzierung sicherstellen).

Die wichtigsten Prozesse für die Durchführung von Programmen zur Sensibilisierung für Informationssicherheit

Die drei Prozesse und die damit verbundenen Teilprozesse können wie folgt dargestellt werden:


A
Planung, Beurteilung und Konzeption
A-010
Vorläufiges Programmteam aufstellen
A-020
Veränderungsmanagement-Konzept entwickeln
A-030
Ziele und Zielvorgaben festlegen
A-040
Zielgruppen bestimmen
A-050
Bedarf an Personal und Sachmitteln für das Programm bestimmen
A-060
Mögliche Lösungen bewerten
A-070
Lösungsansatz auswählen und Auftrag vergeben
A-080
Unterstützung und Mittelbereitstellung durch die Führungsebene sicherstellen
A-090
Arbeitsplan erstellen
A-100
Programm und Aufgabenkatalog ausarbeiten
A-110
Kommunikationskonzept festlegen
A-120
Erfolgsindikatoren für das Programm festlegen
A-130
Ausgangsbasis der Evaluierung bestimmen
A-140
Gewonnene Erfahrungen dokumentieren
B
Ausführung und Abwicklung
B-010
Programmteam bestätigen
B-020
Arbeitsplan überprüfen
B-030
Programm starten und durchführen
B-040
Effizient kommunizieren
B-050
Gewonnene Erfahrungen dokumentieren
C
Evaluierung und Optimierung
C-010
Evaluierung durchführen
C-020
Daten sammeln
C-030
Feedback aus der Kommunikation einbeziehen
C-040
Zielvorgaben des Programms überprüfen
C-050
Gewonnene Erfahrungen anwenden
C-060
Programm gegebenenfalls anpassen
C-070
Programm wiederaufnehmen

Phase I – Planung, Beurteilung und Konzeption



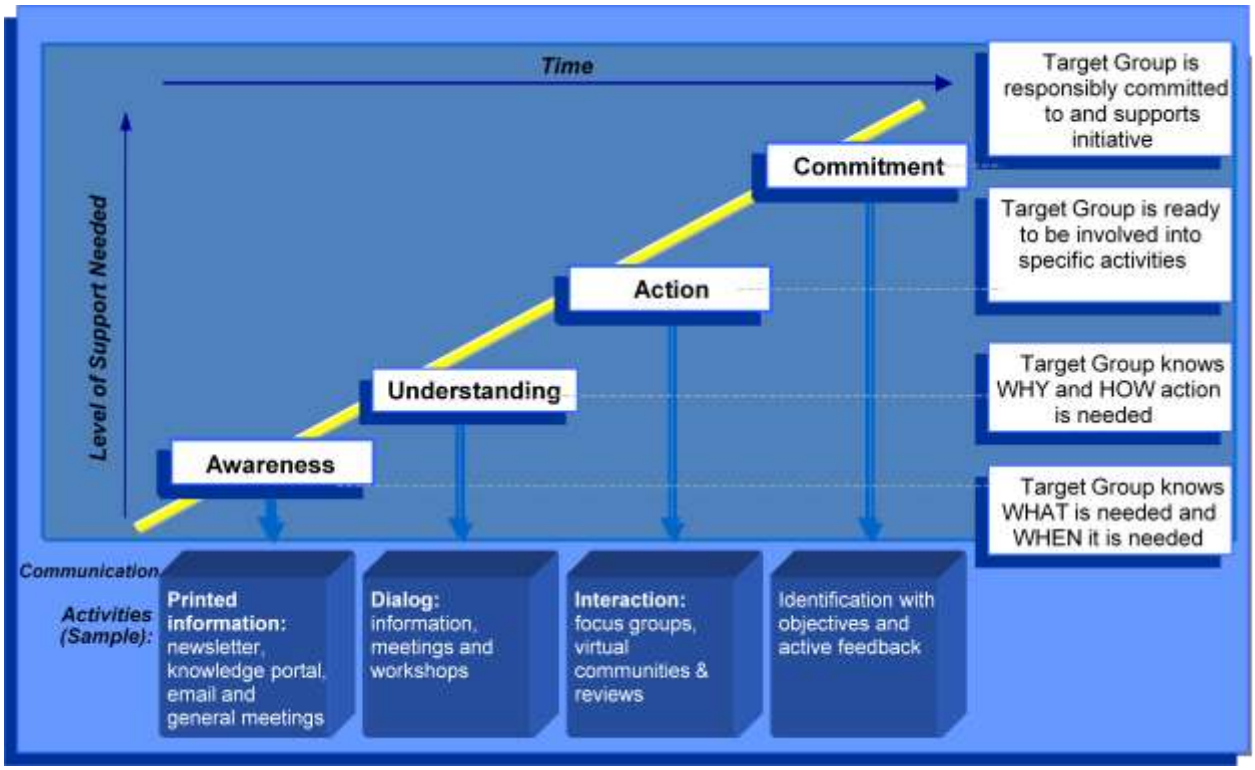
Vorläufiges Programmteam aufstellen

Zunächst muss das Team zusammengestellt werden, das den Prozess zur Planung eines Sensibilisierungsprogramms auf den Weg bringt. Wichtigste Zielsetzung dieses Teams ist die Planung und Organisation der Sensibilisierungsinitiative. Hierzu müssen die in der ersten Phase vorgesehenen Aufgaben abgearbeitet werden.

Aus aktuellen Informationen geht hervor, dass das vorläufige Programmteam in Unternehmen in der Regel zunächst nur aus Mitarbeitern der IT-Abteilung besteht. Dies kann zu Problemen führen, wenn andere Abteilungen, die zum Beispiel für das Risikomanagement, das Personalwesen usw. zuständig sind, nicht von Anfang an in das Projekt eingebunden werden. Diese Gefahr besteht insbesondere in multinationalen Unternehmen und/oder sehr großen Unternehmen. Es muss sichergestellt werden, dass die maßgeblichen Personen von Anfang an einbezogen werden.

Veränderungsmanagement-Konzept entwickeln

Ein Konzept für das Veränderungsmanagement ist für eine Sensibilisierungsinitiative von entscheidender Bedeutung, weil es, selbst im Falle eines Kulturwandels, dazu beiträgt, die Lücke zwischen einer bestimmten Problemstellung und den Reaktionen der Betroffenen auf die Notwendigkeit des Wandels zu schließen.



Legende

Time	Zeit
Level of Support Needed	Grad der erforderlichen Unterstützung
Awareness	Sensibilisierung

Understanding	Verständnis
Action	Aktivität
Commitment	Engagement
Communication Activities (sample):	Kommunikationsaktivitäten (Beispiele):
Printed Information: newsletter, knowledge portal, email and general meetings	Informationen in gedruckter Form: Newsletter, Informationsportal, E-Mail und allgemeine Treffen
Dialog: information, meetings and workshops	Dialog: Information, Treffen und Workshops
Interaction: Focus groups, Virtual communities & reviews	Interaktion: Fokusgruppen, virtuelle Plattformen und Berichte
Identification with objectives and active feedback	Identifikation mit Zielvorgaben und aktives Feedback
Target Group is responsibly committed to and supports initiative	Zielgruppe übernimmt Verantwortung für die Initiative und unterstützt sie
Target Group is ready to be involved into specific activities	Zielgruppe ist bereit, sich an spezifischen Aktivitäten zu beteiligen
Target Group knows WHY and HOW action is needed	Zielgruppe weiß, WARUM und WIE gehandelt werden muss
Target Group knows WHAT is needed and WHEN it is needed	Zielgruppe weiß, WAS WANN zu tun ist

Die Anwendung der wichtigsten Grundsätze des Veränderungsmanagements (u. a. zielgerichtete Kommunikation, Einbindung, Schulung und Evaluierung) trägt maßgeblich dazu bei, dass die Ziele der Sensibilisierungsinitiative erreicht werden; zugleich wird damit eine solide Ausgangsbasis für weitere Programme oder Folgeprogramme geschaffen.

Das Veränderungsmanagement muss umfassend sein, damit gewährleistet ist, dass alle Belange integriert werden und dass durch die Veränderungen ein konkreter und anhaltender Nutzen erreicht wird. Bei einem Konzept für ein Sensibilisierungsprogramm kommt es entscheidend darauf an, dass im Vorfeld die folgenden Grundprinzipien für die geplanten Veränderungen einvernehmlich festgelegt werden:

- ✓ Die wichtigsten Interessengruppen in den Bereichen Entscheidung, Planung, Durchführung und Evaluierung müssten bestimmt und eingebunden werden.
- ✓ In Abstimmung mit diesen Interessengruppen wird ein eindeutiges Ziel festgelegt, das den Endpunkt des Änderungsprozesses bildet.
- ✓ Rollen, Zuständigkeiten und Verantwortungsbereiche werden genau definiert.
- ✓ Die wichtigsten Elemente des Veränderungsprozesses werden miteinander verknüpft und integriert.
- ✓ Risiken müssen aufgezeigt und Hindernisse für Veränderungen deutlich angesprochen werden.
- ✓ Für alle Stufen des Veränderungsprozesses müssen Personen benannt werden, die Führungsverantwortung übernehmen.
- ✓ Informationen werden offen, ehrlich, verständlich und rechtzeitig weitergegeben.
- ✓ Die Vorgehensweise muss im Bedarfsfall den Bedürfnissen der Interessengruppen flexibel angepasst werden können.
- ✓ Der Veränderungsprozess erfordert Ressourcen, Unterstützung und Führung.
- ✓ Der Veränderungsprozess wird durch Schulungs- und Entwicklungsmaßnahmen unterstützt, um einen Verhaltens- und Kulturwandel herbeizuführen.
- ✓ Erfahrungen aus vorangegangenen und laufenden Prozessen werden genutzt, die Fähigkeit zur Veränderung wird aufgebaut und Erfolge werden als solche gewürdigt.

Ziele und Zielvorgaben festlegen

Zu Beginn der konkreten Ausarbeitung eines Programms zur Sensibilisierung für Informationssicherheit muss in jedem Fall festgelegt werden, was mit dem Programm erreicht werden soll. Solange die Zielsetzungen nicht eindeutig festgelegt sind, wird es schwierig sein, ein Programm zu planen und zu organisieren; eine Evaluierung des Programms ist ohne Zielvorgaben gar nicht möglich. Nachfolgend ist eine Reihe von Fragen zusammengestellt, die bei der Festlegung von Zielen und Zielvorgaben für ein Programm hilfreich sind.

***Ziele** und **Zielvorgaben**:*

Um Begriffsverwirrung zu vermeiden: Ziele definieren breit gesteckte Zielvorstellungen, während Zielvorgaben enge Zielgrößen festlegen. Ziele sind allgemeine Absichtserklärungen, Zielvorgaben sind präzise formuliert. Ziele sind nicht fassbar, Zielvorgaben hingegen greifbar. Ziele sind abstrakt, Zielvorgaben konkret. Ziele als solche lassen sich nicht validieren, Zielvorgaben hingegen schon.

Kurz gesagt: „Das Ziel beschreibt, wo wir hinwollen. Zielvorgaben geben die Schritte vor, mit denen wir dahin kommen."

Bei der Festlegung dessen, was mit einer Sensibilisierungsinitiative erreicht werden soll, sollten Sie sich intensiv mit folgenden grundlegenden Fragen befassen:

- ✓ Existiert in Ihrer Organisation bereits ein Programm für Informationssicherheit oder ist dies eine für Ihre Organisation völlig neue Initiative? Möglicherweise gibt es bislang kein anderes Programm für Informationssicherheit, aber vielleicht existieren andere Sensibilisierungsprogramme, die als bewährte und erprobte Beispiele oder als Ausgangspunkt dienen könnten.
- ✓ Liegt der alleinige Schwerpunkt des Programms auf dem Thema Sensibilisierung oder wird es auch Schulungs- und Aufklärungselemente enthalten?
- ✓ Welche konkreten Themen soll das Programm abdecken? Welche damit zusammenhängenden Themen könnten außerdem einbezogen werden?
- ✓ Wie häufig wird der Einzelne durch das Programm angesprochen? Reichen diese Intervalle aus, um das Thema Informationssicherheit im Bewusstsein des Einzelnen wachzuhalten?
- ✓ Wie muss das Informationsniveau (und der Detaillierungsgrad) gehalten sein, damit die Ratschläge von den Zielgruppen als sinnvoll und nützlich wahrgenommen werden? Sollten die Informationen in die Tiefe gehen oder genügt ein Überblick, der eher an der Oberfläche des Themas bleibt?

Wenn diese Fragen geklärt sind, sollten Sie auf weitere Aspekte eingehen:

- ✓ Wird mit dem Pogramm beabsichtigt, die Zielgruppe für das Thema Sicherheit zu „sensibilisieren"? Oder soll das Programm den Einzelnen dazu veranlassen, aufgrund der Sensibilisierung sein Verhalten zu ändern? Experten sind sich darin einig, dass Sensibilisierung zwar einen wichtigen Aspekt darstellt, jedoch nicht Endziel des Programms sein sollte. Der Programmplan sollte ein über die reine Sensibilisierung hinausgehendes Ziel verfolgen.
- ✓ Besteht Ihr Ziel darin, ganz generell für das Thema Sicherheit zu sensibilisieren oder wollen Sie gezielt Informationen zu konkreten Problemen vermitteln (und gegebenenfalls

Schulungsmaßnahmen durchführen) oder streben Sie eine Kombination beider Ziele an? Ist die Liste der konkreten Probleme oder Themen bereits festgelegt oder wird sie sich im Verlauf der kommenden Monate und Jahre ergeben? Anhand der Antworten auf diese Fragen können Sie feststellen, ob ein einmalig durchgeführtes Programm ausreicht oder ob eine längerfristig angelegte Initiative erforderlich ist, um zu vermeiden, dass die Zielgruppe überfordert und/oder abgeschreckt wird.

- ✓ Als weiterer Aspekt zur vorhergehenden Frage: Soll das Sensibilisierungsprogramm längerfristig angelegt sein oder ist es als einmalige Kampagne oder eine ähnliche kurzfristige Aktion gedacht, die auf ein bestimmtes Thema ausgerichtet ist? Beide Ansätze haben ihre Vorzüge, sofern sie die jeweiligen Gegebenheiten berücksichtigen, in manchen Fällen erscheint aber auch eine Kombination beider Ansätze angebracht.
- ✓ Wie wird die Initiative durchgeführt? Wird sie in die Arbeit der Organisation eingebunden? Oder wird die Durchführung extern vergeben? Wird ein Projektteam zusammengestellt? Wer übernimmt die Verantwortung? Über welche Qualifikationen/Erfahrungen verfügen die Teammitglieder in den Bereichen Informationssicherheit und sicherheitsbezogene Sensibilisierung/Schulung/Aufklärung? Welche Rollen und Verantwortungsbereiche werden den einzelnen Personen zugewiesen?

Eine realistische Einschätzung des Aufwands an Zeit und Ressourcen für die Planung und Durchführung des Programms macht sich mit Sicherheit bezahlt.

Bedenken Sie bei der Festlegung von Zielen und Zielvorgaben, dass möglicherweise nicht genügend Mittel für die sachgerechte Durchführung des Programms zur Verfügung stehen werden, und treffen Sie entsprechende Vorkehrungen für einen solchen Fall.([13]) Im Abschnitt „Finanzierung sicherstellen" werden einige Szenarien beschrieben, die Hinweise und Ideen liefern, wie Sie ein Sensibilisierungsprogramm mit begrenzten finanziellen Mitteln durchführen können, ohne auf die wesentlichen Elemente einer erfolgreichen Initiative verzichten zu müssen.([14])

Zielgruppen bestimmen

Es ist wichtig, das spezifische Zielpublikum der Sensibilisierungsinitiative genau zu bestimmen. Folgende Fragen können dabei helfen:

- ✓ Wer soll mit dem Sensibilisierungsprogramm erreicht werden?
- ✓ Haben alle Zielgruppen die gleichen Bedürfnisse oder ist ihr Informationsbedarf unterschiedlich? Gibt es einzelne Zielgruppen, die einen völlig anderen Informationsbedarf haben?
- ✓ Haben alle Zielgruppen den gleichen Kenntnisstand oder verfügen sie über unterschiedliche Kenntnisse?
- ✓ Mit welcher Form der Kommunikation lässt sich die Botschaft des Sensibilisierungsprogramms am besten vermitteln?
- ✓ Wie stehen die Zielgruppen zur Kultur der Informationssicherheit? Wird das Thema von ihnen im Allgemeinen ernst genommen oder halten sie es für weniger wichtig? Hatten die Angehörigen der Zielgruppen in der Vergangenheit bereits mit Handlungsempfehlungen oder Verfahrensanleitungen zum Thema Informationssicherheit zu tun? Wenn ja, werden die

([13]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.
([14]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

betreffenden Unterlagen gepflegt und aktualisiert oder müssen sie im Rahmen des Sensibilisierungsprogramms entwickelt und bekannt gemacht werden?

Das spezifische Zielpublikum, das durch das Sensibilisierungsprogramm angesprochen werden soll, muss im Vorfeld bestimmt werden. Es empfiehlt sich, die betreffenden Informationen in einem geeigneten Formular zu erfassen. Anhang I enthält eine Vorlage zur Erfassung von Zielgruppendaten.

Beispiele für mögliche Zielgruppen von Initiativen und Programmen zur Sensibilisierung für Informationssicherheit:

Nr.	Zielgruppe	Beschreibung
1	Private Nutzer	Bürger jeden Alters mit unterschiedlichem technischem Kenntnisstand, die IKT außerhalb der Arbeit für private Zwecke nutzen. Diese Nutzergruppe lässt sich in weitere Gruppen untergliedern: Kinder, Teenager, Jugendliche, Erwachsene und ältere Menschen, die sogenannten „Silver Surfer".
2	Arbeitnehmer	Das gesamte Personal einer Organisation.
3	Führungskräfte der mittleren Führungsebene	Führungskräfte aus allen Bereichen der Organisation, die für die Arbeit und Leistung des Personals verantwortlich sind. Diese Gruppe, die häufig nur über geringe technische Kenntnisse verfügt, muss geschult werden und die Bedeutung der Informationssicherheit erkennen. Dies gewährleistet, dass sie die entsprechenden Sicherheitsmaßnahmen und -kontrollen in ihren Geschäftsbereichen durchführen können.
4	Oberste Führungsebene	Die Führungskräfte der obersten Führungsebene sind die wichtigsten Entscheidungsträger für Investitionen in Informationssicherheit.
5	Systemadministratoren	Mit technischen Aufgaben befasste Mitarbeiter, die in der Regel für die Einrichtung und Sicherheit von Netzwerkservern und Sicherheitssystemen verantwortlich sind.
6	Dritte	Partner, Lieferanten, Berater, die mit der Durchführung bestimmter Aufgaben in einer Organisation beauftragt werden. Gartner verweist in einer Veröffentlichung darauf, dass ein neuer massiver Verstoß gegen die Datensicherheit in Kalifornien deutlich macht, dass Unternehmen ihre externen Auftragnehmer zu strengeren Sicherheitsmaßnahmen verpflichten müssen.([15])

([15]) Girard, John, und Litan, Avivah, *New data loss highlights problems with contractors and laws,* Gartner, 4. Februar 2008.

7	.....	

Bei der Konzeption eines Sensibilisierungsprogramms ist es entscheidend, dass alle Rollen genau definiert werden. Das RACI-Modell([16]) erleichtert diese Aufgabe. Die nachfolgende Grafik zeigt ein Beispiel des RACI-Modells, bei dem in der linken Spalte die Tätigkeiten und in der Kopfzeile die Funktionen angegeben sind, die für die Durchführung der Initiative zuständig oder daran beteiligt sind.

	Führungsebene	**IT-Sicherheits-beauftragter**	**Personalabteilung**	**Mitarbeiter und Auftragnehmer**	**....**
Tätigkeit 1	AR	C	I	I	...
Tätigkeit 2	A	R	C	I	...
Tätigkeit 3	I	A	I	I	...
Tätigkeit *n*	I	A	C	I	...

Bedarf an Personal und Sachmitteln für das Programm bestimmen

In dieser Phase ist es an der Zeit, den Bedarf an Personal und Sachmitteln für das Programm zu bestimmen. Zunächst sollte dabei festgestellt werden, ob innerhalb der Organisation entsprechende Ressourcen vorhanden sind. Mitarbeiter aus den Bereichen IT, Personalwesen, Kommunikation, Aus- und Weiterbildung und Entwicklung verfügen am ehesten über den geeigneten fachlichen und Erfahrungshintergrund für die Mitwirkung an einem Sensibilisierungsprogramm.

Mit Blick auf die benötigten Sachmittel und das erforderliche Erfahrungswissen könnten sich Ratschläge und Erfahrungen von Kollegen und/oder Organisationen, die mit der Abwicklung von Sensibilisierungs-, Schulungs- oder Aufklärungsprogrammen vertraut sind, als besonders hilfreich erweisen. Zudem empfiehlt sich im Sinne der Einbindung von Interessengruppen die Kontaktaufnahme, wenn in einer späteren Phase die Unterstützung dieses Personenkreises für die Durchführung des Programms benötigt wird. Wer auf die Einbindung von Kollegen verzichtet, läuft Gefahr, dass diese sich übergangen fühlen und daher – möglicherweise unbewusst – gegen das Programm opponieren.

Das Internet bietet ein breites Spektrum an Informationen und Material, die kostenlos oder gegen Gebühr abgerufen werden können. Zahlreiche kostenlos zugängliche Foren und Plattformen widmen sich speziell der Sensibilisierung für Sicherheitsbelange. Die Mitgliedschaft in solchen Foren und Plattformen könnte sich als durchaus nützlich erweisen, zumal Mitglieder Zugang zu den jeweiligen Archiven erhalten. In diesem Zusammenhang wird darauf hingewiesen, dass die ENISA im Februar 2008 eine Plattform für die Zusammenarbeit bei der Sensibilisierung eingerichtet hat.

Zwar lassen sich Informationen über Produkte und Dienstleistungen zum Thema in nahezu beliebiger Menge problemlos beschaffen, doch kommt es bei der Informationsbeschaffung darauf an, systematisch vorzugehen, da dies das weitere Vorgehen wesentlich erleichtert.

Nach der Informationssammlung steht eine gründliche Sichtung der Liste der internen und externen Ressourcen an. Hierbei sollte besonders darauf geachtet werden, diejenigen Elemente herauszufiltern, die für das Programm von Nutzen sein könnten und sich in das Programm einfügen.

([16]) RACI, das Akronym für die englischen Begriffe „responsible, accountable, consulted, informed", steht für „zuständig, verantwortlich, beratend, informiert".

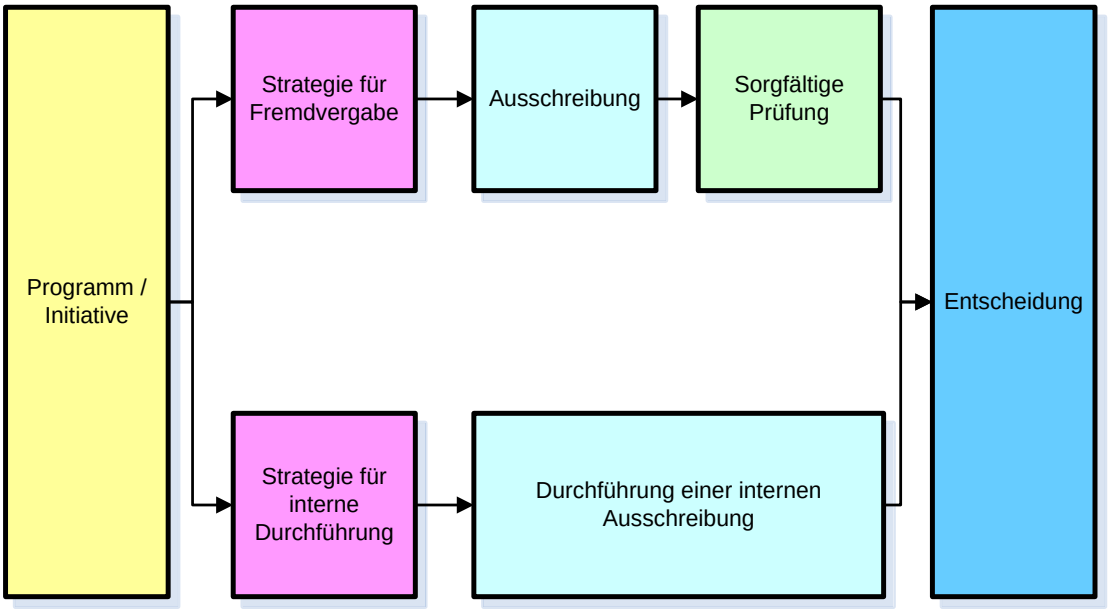
Informationen, die auf den ersten Blick nicht nutzbringend erscheinen, werden häufig vernachlässigt, doch ist hier Vorsicht geboten. Oft werden nützliche Ressourcen übersehen, weil sie nicht ausführlich genug dargestellt oder – im Falle gewerblicher Dienstleistungsangebote – schlecht vermarktet werden.

Als letzter Schritt in dieser Phase wird eine Liste der in die engere Wahl genommenen Lösungen erstellt, die dann in der nächsten Phase einer Bewertung unterzogen werden.

Mögliche Lösungen bewerten

Bei der Bewertung möglicher Lösungen ist zunächst die Frage zu stellen, ob das Sensibilisierungsprogramm intern durchgeführt oder extern vergeben wird. Im Zuge strategischer Überlegungen geht der Trend in Richtung Fremdvergabe. Unternehmen und Institutionen können heute besser einschätzen, wo ihre Stärken liegen und welche Aufgaben von externen Partnern effektiver erledigt werden können. Damit steht die Entscheidung an, ob eine Aufgabe extern vergeben werden soll, welche Aufgabengebiete fremdvergeben werden können, wie die Vergabe vertraglich gestaltet werden soll und wie geeignete Partner gefunden werden, um den Erfolg von Programmen und Initiativen nicht zu gefährden.

Das nachstehende Ablaufdiagramm veranschaulicht die beispielhafte Vorgehensweise im Entscheidungsprozess über interne Durchführung oder Fremdvergabe. Es empfiehlt sich, auch wenn das Programm nicht extern vergeben wird, eine interne Ausschreibung durchzuführen, weil dieser Prozess durch seine Stringenz das Programmteam dazu zwingt, die eigenen Anforderungen straff zu strukturieren.



Entscheidungsprozess – interne Durchführung oder Fremdvergabe

Der komplette Prozess der Evaluierung und Bewertung folgt dem gängigen Ausschreibungsverfahren:

1. Offizielle Ausschreibung mit den aus den beiden ersten Phasen des Prozesses abgeleiteten genauen Anforderungen ausarbeiten. Die Besetzung des Programmteams muss festgelegt werden, ebenso die geforderten Erfahrungen und Eigenschaften, Rollen und Verantwortungsbereiche sowie die hierarchischen Strukturen.
2. Verfahren und Strategien des Programms müssen festgelegt und formalisiert werden. Dies schließt Vorgaben für wöchentliche Statusberichte, Finanzberichte und Problembehandlung ein.
3. Ausschreibung mit Angebotsfrist an potenzielle Bieter versenden.
4. Eingegangene Fragen der Bieter zusammenstellen und Antworten fristgerecht allen Bietern zukommen lassen, ohne dabei die Herkunft der Fragen offenzulegen.
5. Nach Ablauf der Angebotsfrist keine weiteren Angebote annehmen; mit der systematischen Auswertung und Bewertung anhand des zuvor erstellten Aufgabenkatalogs beginnen.
6. Die Angebote zunächst auf die Einhaltung der wesentlichen Anforderungen prüfen; auf diese Weise können Bieter, die diese Anforderungen nicht beachtet haben, von vornherein ausgeschlossen werden.
7. Auch zusätzliche Angebote der Bieter prüfen – sie enthalten unter Umständen nützliche Aspekte und hilfreiche Ideen, die bis dahin übersehen wurden. Sie können gegebenenfalls auch als Entscheidungshilfe herangezogen werden, wenn mehrere Bieter in der Bewertung dicht beieinanderliegen.
8. Aufschluss über Professionalität und Qualität der Bieter verschafft eine Prüfung der Qualität der Angebote und der im Angebot angeführten Referenzsysteme und -materialien.
9. Die Wertnoten der einzelnen Bieter berechnen (Gesamtnote aus (Wertnote für jedes Kriterium x Gewicht des betreffenden Kriteriums) geteilt durch die erreichbare Höchstpunktzahl x 100 %).
10. Wenn entschieden wurde, das Programm (ganz oder teilweise) extern zu vergeben, sollten zum Ausschreibungsverfahren unbedingt Fachleute aus dem Einkauf hinzugezogen werden, die für eine faire Abwicklung des Verfahrens sorgen.
11. Wird das Programm intern vergeben, kann es wesentlich zu einer integrativen und transparenten Atmosphäre beitragen, wenn alle Entscheidungen, die das Programm betreffen, in einem Ausschuss getroffen werden.

Bereits bei der Festlegung der Anforderungen (Punkt 1 oben) ist zu überlegen, wie später die Effektivität des Programms evaluiert werden soll.

Wenn die Maßnahme von einem externen Anbieter durchgeführt wird, muss sichergestellt werden, dass das Sensibilisierungsprogramm und das Material auf die Erfordernisse der Organisation abgestimmt werden. Es ist zum Beispiel nicht empfehlenswert, ein Standardmodul oder Standardmaterial für die Schulung einzusetzen oder das Sensibilisierungsprogramm für ein bestimmtes Thema von einer anderen Organisation zu übernehmen. Programme zur Sensibilisierung für Informationssicherheit sollten auf das Tätigkeitsumfeld der Organisation abgestimmt werden.([17])

([17]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

Die Ausschreibung muss präzise formulierte Anforderungen enthalten. Anhang II enthält ein Muster für eine Ausschreibung. Außerdem müssen in diesem Stadium Verfahren und Vorschriften (Wochenberichte usw.) festgelegt und formalisiert werden. Anhang III enthält eine Vorlage für einen wöchentlichen Statusbericht.

Lösungsansatz auswählen und Auftrag vergeben

Es ist denkbar, dass am Ende der Bewertung kein eindeutiger Sieger der Ausschreibung feststeht, sondern dass vielmehr beschlossen wird, Teile des Programms intern durchzuführen, während andere Teile an einen oder mehrere externe Bieter vergeben werden. Auch Verhandlungen, bei denen es beispielsweise um die genauere Klärung von Budget, Preis und Konditionen sowie darum geht festzulegen, was vom Auftragnehmer in welchem Zeitrahmen vorzulegen ist, sind Teil des Auswahlverfahrens.

In dieser Phase ist es wichtig, bei der Auswahl des Lösungsansatzes den Nutzen des Programms zu berücksichtigen.
Am Ende dieses Prozesses wird eine Entscheidung getroffen, der Auftrag erstellt und der Vertrag unterzeichnet.

Den Nutzen des Programms herausstellen

Damit die Führungsebene für die Bereitstellung von Unterstützung und Finanzmitteln gewonnen werden kann, müssen der Nutzen bzw. die Vorteile des Programms herausgestellt werden.

Ein Programm zur Sensibilisierung für Informationssicherheit bietet folgenden Nutzen:

- ✓ Es dient als Fokus und Impulsgeber für verschiedene Sensibilisierungs-, Schulungs- und Aufklärungsmaßnahmen zum Thema Informationssicherheit, die zum Teil vielleicht bereits existieren, die jedoch möglicherweise besser koordiniert und effektiver gestaltet werden müssen.
- ✓ Es dient der Weitergabe maßgeblicher Handlungsempfehlungen oder Verfahrensanleitungen, die für die Sicherheit von Informationsressourcen wichtig sind.
- ✓ Es vermittelt Adressaten in Schlüsselfunktionen grundlegende, aber auch spezielle Informationen über Gefahren für die Informationssicherheit und über Möglichkeiten zu deren Kontrolle.
- ✓ Es macht den Einzelnen auf seine persönliche Verantwortung im Hinblick auf die Informationssicherheit aufmerksam.
- ✓ Es motiviert den Einzelnen dazu, Handlungsempfehlungen und Verfahrensanleitungen ernst zu nehmen.
- ✓ Es schafft eine tragfähigere Sicherheitskultur, die auf fundierten Kenntnissen und dem Engagement aller Beteiligten für Informationssicherheit basiert.

- ✓ Es trägt dazu bei, die Einheitlichkeit und Wirksamkeit der bestehenden Kontrollmechanismen für Informationssicherheit zu verbessern und setzt im besten Fall Anreize für die Einführung kostenwirksamer Kontrollmechanismen.
- ✓ Es trägt dazu bei, dass Zahl und Ausmaß von Verstößen gegen die Informationssicherheit auf ein Minimum beschränkt bleiben, und leistet damit einen Beitrag zur Kostensenkung – direkt (z. B. durch die Vermeidung von Datenverfälschungen durch Viren) und indirekt (z. B. weniger Aufwand für die Untersuchung und Aufklärung von Sicherheitsverstößen). Dies stellt den wichtigsten finanziellen Nutzen des Programms dar.

Unterstützung und Mittelbereitstellung durch die Führungsebene sicherstellen

Der vielleicht kritischste Aspekt der gesamten Initiative besteht darin, die Führungsebene von dem Sensibilisierungsprogramm zu überzeugen und ihre Unterstützung für das Programm zu gewinnen.([18]) Es ist unbedingt erforderlich, dass sich die Entscheidungsträger darüber einig sind, dass das Sensibilisierungsprogramm wichtig ist und eine entsprechende Mittelausstattung verdient.

Hier greift das Konzept der IT-Governance, also der guten IT-Verwaltung. Wenn es nicht gelingt, den wichtigsten Interessengruppen verständlich zu machen, dass ein Programm zur Sensibilisierung für Informationssicherheit zwingend erforderlich ist, und sie von den Zielen und Zielvorgaben zu überzeugen, dann wird die Initiative wegen des passiven Widerstands der Beteiligten im Ansatz stecken bleiben. Daher muss vor der Durchführung einer Initiative oder eines Programms allen Beteiligten deutlich gemacht werden, dass ihre Mitwirkung von zentraler Bedeutung ist.

([18]) ENISA, *Unterstützung und Mittelbereitstellung durch die Unternehmensleitung*, 2008; Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005;
IT Governance Institute, *Information security governance: Guidance for boards of directors and executive management*, Second Edition, USA, 2006.

Internationales Versicherungsunternehmen — das Engagement der Führungsebene als Erfolgsfaktor

Ein Versicherungsunternehmen erklärte, weshalb die Informationssicherheit für seine Geschäftstätigkeit wichtig ist. Es sammelt, speichert und verarbeitet erhebliche Mengen an finanziellen, medizinischen und personenbezogenen Informationen. Diese Informationen sind sein wichtigster Vermögenswert; eine Verletzung der Geheimhaltungspflicht könnte den Ruf des Unternehmens schädigen und Auslöser für Rechtsstreitigkeiten sein. Unglücklicherweise treten jedoch Bedrohungen (wie der Diebstahl personenbezogener Daten und Betrügereien) immer häufiger auf, daher ist es wichtig, die Mitarbeiter für die Gefahren zu sensibilisieren.

Die größte Herausforderung bestand in der Entwicklung eines Konzepts, das für über 10 000 Mitarbeiter geeignet ist, die noch dazu verschiedene Sprachen sprechen. Eigens hierfür engagierte das Unternehmen einen externen Anbieter, der das Unternehmen bei der Erstellung passender Schulungspläne und -materialien unterstützen sollte. Um die Mitarbeiter wirksam zu erreichen, wurden die Schulungsunterlagen in die Sprachen der betreffenden Länder übersetzt.

Es gibt ein fortlaufendes Programm zur Anpassung und Vermittlung der Kernbotschaften. Ziel des Programms ist es, das Verhalten der Mitarbeiter und deren Wahrnehmung von Risiken zu ändern. Um das Zielpublikum zu erreichen, werden verschiedene Techniken eingesetzt, da unterschiedliche Menschen unterschiedlich lernen.

Als wirksamste Methode hat sich der direkte Kontakt zu den Mitarbeitern in Form von Workshops und Schulungen erwiesen. Wenn man einen Namen oder eine Funktion mit einem Gesicht verbinden kann, entsteht ein persönlicherer Bezug und Botschaften werden in der direkten Ansprache besser aufgenommen. Die Teilnahme an den Schulungen ist verpflichtend. Die Führungsebene unterstützt die Sensibilisierungsmaßnahmen aktiv, sorgt dafür, dass die Schulungen zu für das Unternehmen geeigneten Zeiten stattfinden, und wirbt unter den Mitarbeitern für die Veranstaltung. Die Schulungen werden gut besucht; wenn Mitarbeiter nicht daran teilnehmen, wird dies den Vorgesetzten gemeldet. Die unternehmensweite Unterstützung durch die Führungsebene hat sich als wesentlicher Faktor für den Erfolg des Sensibilisierungsprogramms erwiesen.

Andere, nicht interaktive Mechanismen wie Beiträge im Intranet, E-Mails, Plakate und Veröffentlichungen werden eingesetzt, um wichtige Botschaften zu verstärken. Es hat sich jedoch als schwierig erwiesen zu beurteilen, wie viele Mitarbeiter die Botschaften gelesen oder verstanden haben; zudem können sie leicht ignoriert werden. Diese Formen der Vermittlung dienen daher eher als Ergänzung denn als Ersatz für traditionelle Schulungen.

Wichtigstes Messinstrument für die Wirkung der Sensibilisierungsschulungen sind Rückmeldungen und Fragebogen, die am Ende der Schulungen oder kurz danach ausgefüllt werden. Diese Rückmeldungen vermitteln einen guten Eindruck von der Wirkung der Schulungen auf den einzelnen Mitarbeiter. Im Allgemeinen fallen sie positiv aus – die Mehrheit der Teilnehmer gibt an, dass sie Neues gelernt haben und dass sie sich bemühen werden, ihr Verhalten zu ändern.

Telekommunikationsanbieter — Austausch mit den Mitarbeitern

Die IT-Systeme eines Telekommunikationsanbieters sind für die Bereitstellung der Dienstleistungen für seine Kunden unverzichtbar. Jedes Problem mit der Informationssicherheit könnte in kurzer Zeit dem Ruf des Unternehmens schaden. Ein Schulungsprogramm zur Sensibilisierung für Sicherheitsbelange sollte daher ein Anliegen der obersten Ebene sein.

In diesem internationalen Unternehmen bestand der erste Schritt darin, die Unterstützung der lokalen Unternehmensführung für die Kernbotschaften zu gewinnen. Letztendlich hat der persönliche Austausch der Führungskräfte mit den Mitarbeitern die größten Auswirkungen auf das Verhalten. Die Unterstützung der richtigen Personen zu gewinnen, ist für den Erfolg des Programms entscheidend.

Das Unternehmen beschäftigt eine Vielzahl verschiedener Menschen mit unterschiedlichem Kenntnissen und unterschiedlichen Schulungsbedürfnissen. Ein zentrales Team entwickelt die grundlegenden verbindlichen Leitlinien und Schulungen, die eine einheitliche und konsistente Botschaft beinhalten. Dazu gehören E-Learning-Module und Quizspiele. Zusätzliche Informationen und optionales Schulungsmaterial sind ebenfalls vorhanden. Dadurch sind die lokalen Unternehmenseinheiten in der Lage, Sicherheitsvorschriften und -schulungen für Gruppen an die lokalen Gegebenheiten und die Bedürfnisse der Mitarbeiter anzupassen. Das zusätzliche Material umfasst Plakate, Bildschirmschoner und Quizspiele.

Alle Informationen sind über ein globales Sicherheitsportal zugänglich. Dieses hat sich als wirksamste Methode erwiesen, Informationen weltweit zu verbreiten. Der Zugang zum Portal ist für die Benutzer einfach und nimmt wenig Zeit in Anspruch. Das zentrale Team kann die Inhalte leicht aktualisieren.

Auf Länderebene hat sich die persönliche Diskussion von Themen unter Mitarbeitern als die beste Methode zur stärkeren Sensibilisierung erwiesen. Hierfür werden sowohl Einführungs- als auch Weiterbildungsschulungen eingesetzt.

Für jeden wichtigen Geschäftsbereich werden vor größeren neuen Initiativen regelmäßig Sicherheitsrisikobewertungen und Schwachstellenanalysen durchgeführt. Deren Ergebnisse werden dazu verwendet, die Schulungen und die Botschaften weiter zu verbessern und die Effektivität der Maßnahme zu messen.

In kontinuierlich durchgeführten Mitarbeitererhebungen wird der Stand des Sicherheitsbewusstseins ermittelt. Einmal pro Jahr werden die Ergebnisse analysiert, um Verhaltensänderungen festzustellen. Diese Analyse wird dann mit der Risikobewertung und der Schwachstellenanalyse verglichen, um Wirkung und Effektivität des Programms zu bewerten.

Zunächst gilt es herauszufinden, was den einzelnen Interessengruppen wichtig ist und welche Themen für sie einen besonders hohen Stellenwert haben. Ausgehend davon sollten dann alle Beteiligten während der gesamten Laufzeit in das Programm eingebunden werden. Wenn ein Programm von denjenigen Akteuren, die die Ressourcen bereitstellen, und denjenigen, die die Programmergebnisse nutzen, nicht akzeptiert wird, ist sein Erfolg zumindest infrage gestellt. Es ist daher wichtig, eine Interessen- und Unterstützungsgemeinschaft für das Programm aufzubauen. Die Bedeutung der Einbindung von Interessengruppen in ein Projekt, ein Programm oder eine Initiative darf keinesfalls unterschätzt werden.

Je nach Unternehmen oder Institution muss gegebenenfalls eine solide finanzielle Begründung für die Investition ausgearbeitet werden. In jedem Fall lassen sich die Vorzüge eines Sensibilisierungsprogramms umso überzeugender der obersten Führungsebene darstellen, je eindrucksvoller sie durch entsprechende Zahlen und Fakten untermauert werden. Der Aufbau eines Geschäftsszenarios hat wesentlichen Einfluss auf den Erfolg einer Sensibilisierungsinitiative.

Durch umfassendere und präzise definierte Kooperationen oder Partnerschaften, beispielsweise in Form von öffentlich-privaten Partnerschaften oder länderübergreifenden Initiativen, lässt sich die potenzielle Reichweite einer Kampagne maximieren. Öffentlich-private Partnerschaften erweisen sich bei der Durchführung von Kampagnen nicht selten dadurch als besonders effektiv, dass jede Organisation ihre besonderen Stärken und ihre Ressourcen gezielt einbringen kann. Für ein Gemeinschaftsprogramm sollten verbindliche Verhaltensregeln (oder eine Satzung) und gemeinsame Elemente wie Planungsleitfäden erarbeitet werden. Im organisatorischen Bereich sollte eine öffentlich-private Partnerschaft so angelegt sein, dass eine Lenkungsgruppe, ein Projektmanagementteam, eine Arbeitsgruppe (die auch für Medienkontakte zuständig ist) sowie Teams für untergeordnete Projekte vorhanden sind.

Staatliche Stellen — Verhaltensregeln sind unverzichtbar

Eine Behörde erläutert, warum Verhaltensregeln immer wichtiger werden und zunehmend in öffentlich-privaten Partnerschaften eingesetzt werden. Die Behörde will sicherstellen, dass jede Sensibilisierungsinitiative als wichtiger Schritt zur Gewährleistung der Online-Sicherheit angesehen wird.

Besonders schwierig ist eine ausgewogene Gestaltung des Inhalts. Der Zweck öffentlich-privater Partnerschaften besteht nicht in der Absatzförderung für ein Produkt oder eine Dienstleistung, sondern darin, die Nutzer aufzuklären und eine Änderung ihres Verhaltens zu erreichen. Es ist wichtig, dass Staat und Wirtschaft gemeinsam einen einheitlichen Ansatz zur Förderung der Sicherheit im Internet verfolgen.

Finanzierung sicherstellen

Es gibt verschiedene Methoden, wie Unternehmen die Finanzierung sicherstellen und die Mittelverwaltung insgesamt gestalten können. Die Verfahren, die von den Organisationen zur Finanzierung von Initiativen zur Sensibilisierung für Informationssicherheit angewandt werden, sind sehr unterschiedlich. Im Folgenden einige Beispiele:([19])

- ✓ Bereitstellung eines prozentualen Anteils der Mittel, die eine Organisation für Schulungen aufwendet
- ✓ Bereitstellung eines prozentualen Anteils der Mittel, die eine Organisation für den Bereich Informationstechnologie aufwendet
- ✓ Jeder Geschäftsbereich stellt einen prozentualen Anteil seines Budgets bereit, der sich nach der Zahl seiner Mitarbeiter richtet

([19]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

- ✓ Bereitstellung eines Pauschalbetrags je Nutzer entsprechend der Rolle und der Teilnahme am Schulungsprogramm
- ✓ Bereitstellung eines Pauschalbetrags, unabhängig von den Zielen und Zielvorgaben der Sensibilisierungsmaßnahmen
- ✓ Bereitstellung bestimmter Beträge für die festgelegten Ziele und Zielvorgaben der Sensibilisierungsmaßnahmen

Die Mittelzuweisung ist bereits erfolgt

Wenn die Mittelzuweisung bereits erfolgt ist, kann es erforderlich sein, die Durchführbarkeit der festgelegten Ziele und Zielvorgaben der Sensibilisierungsinitiative nochmals zu überprüfen. Mit einem zu knapp bemessenen Budget können unter Umständen nicht alle Ziele und Zielvorgaben der Sensibilisierungsmaßnahme erreicht werden. Deshalb sollten diejenigen Ziele und Zielvorgaben Priorität erhalten, die als für das Programm wesentlich angesehen werden.

Auch die Beantragung weiterer Mittel ist eine Möglichkeit, die in Betracht gezogen werden kann.

Finanzierungsplan aufstellen

Im besten Fall wird zunächst die Sensibilisierungsstrategie festgelegt und dann das für die Umsetzung der festgelegten Ziele und Zielvorgaben erforderliche Budget bestimmt. Der letzte Teil der Aufgabe besteht nun darin, die Kosten zu ermitteln, die mit der Initiative verbunden sind. Dies geschieht im Rahmen der nächsten Tätigkeit.

Kosten ermitteln

Für die erfolgreiche Durchführung eines Sensibilisierungsprogramms müssen zunächst die benötigten Mittel beantragt werden. Dazu ist es notwendig, sowohl die Festkosten als auch die variablen Kosten für eine Sensibilisierungsinitiative zu ermitteln. Nachfolgend einige Beispiele.

Kosten	Festkosten	Variable Kosten
1. Personal und freie Mitarbeiter	Personal	Berater, freie Mitarbeiter
2. Betriebskosten	Miete	
	Website-Betreuung	
		Informationsmaterial
	Sonstige Bürokosten	
3. Werbung und Bekanntmachung		Kosten von Werbematerial
		Kosten der Verbreitung von Werbematerial
		Gestaltungskosten der Werbung
		Medienkosten der Werbung
4. Schulung		Individuelle Materialkosten
		Kosten für Schulungsräume pro Veranstaltung

Beispiele

Der Hauptteil der Kosten entfällt hierbei auf das Team, das für die Durchführung des Programms zur Sensibilisierung für Informationssicherheit zuständig ist. Wenn intern genügend Personal mit einschlägigen Fachkenntnissen vorhanden ist, müssen entsprechende Mitarbeiter für die Initiative abgestellt werden. Ansonsten sind bei den Kosten das Gehalt eines Programmleiters und zusätzliche Personalkosten für die Mitarbeiter des Programmteams einschließlich entsprechender Nebenkosten einzurechnen, außerdem die Kosten für Entwicklung, Herstellung und Verbreitung der Materialien

zum Thema Sensibilisierung, die Kosten für externe Schulungskurse und Schulungsräume usw. Die typischerweise anfallenden Kosten lassen sich wie folgt zusammenfassen:

- ✓ Leiter des Programms für Informationssicherheit und Programmmitarbeiter (Vollzeit oder Teilzeit – Gehälter und Sozialleistungen, gegebenenfalls zuzüglich Personalbeschaffungskosten)
- ✓ Informationsmaterial (Abonnements bei einschlägigen Fachfirmen wie Gartner, IsecT usw.), soweit nicht bereits vorhanden
- ✓ Werbematerial (themenspezifische Materialien wie Bildschirmschoner, Kugelschreiber, Plakate, Mousepads, Gewinnspiele usw.)
- ✓ Druckkosten (für alle Materialien, die nicht auf elektronischem Wege verschickt werden)

Bei der Zusammenstellung der Kosten einer Initiative sollte auch der mögliche Beitrag Dritter berücksichtigt werden. Dies gilt vor allem dann, wenn ein Programm zur Sensibilisierung für Informationssicherheit im Rahmen einer öffentlich-privaten Partnerschaft durchgeführt wird.

Geschäftsszenario erstellen

Zwar sind die Sicherheitsausgaben in den letzten Jahren gestiegen, doch hat sich an den Verfahren zur Rechtfertigung dieser Ausgaben kaum etwas geändert. Nach Angaben des Ministeriums für Wirtschaft, Unternehmen und Regelungsreform (Department for Business, Enterprise and Regulatory Reform, BERR) im Vereinigten Königreich erstellen 48 % aller großen Unternehmen grundsätzlich und 41 % dieser Unternehmen gelegentlich ein Geschäftsszenario für Sicherheitsausgaben. Bei den Unternehmen, die grundsätzlich ein Geschäftsszenario erstellen, wird meist auch der Nutzen erfasst (32 %), während nur ein geringer Teil dieser Gruppe (16 %) die Rentabilität bewertet.([20]) Der Grund hierfür könnte darin bestehen, dass ihr guter Ruf, der ihr größtes Kapital ist, nur schwer zu quantifizieren ist.

Die Erstellung eines Geschäftsszenarios lohnt sich, da der Anteil des IT-Budgets, der für Sicherheitsausgaben aufgewendet wird, auf durchschnittlich 9-10 % geschätzt wird.([21])

Die Erstellung eines überzeugenden Geschäftsszenarios, das der Führungsebene vorgestellt wird und in dem der quantitative und der qualitative Nutzen von Sensibilisierungsprogrammen aufgezeigt werden, bildet auch die Grundlage für eine erfolgreiche Sensibilisierungsinitiative. Geschäftsszenarien verbessern die Chancen eines erfolgreichen Projekts, weil sie der Führungsebene Aufschluss über den Wert der Investitionen geben und ihr eine fundierte Entscheidung über die Finanzierung verhelfen. Aufgrund ihrer Glaubwürdigkeit bewirken sie zudem ein Engagement der Akteure, das über eine bloße Unterstützung hinausgeht, und sie dienen als Orientierungshilfe für die Arbeit, um sicherzustellen, dass der erwartete Nutzen tatsächlich erreicht wird.

Weitere Formen von Geschäftsszenarien sind auch Kosten-Nutzen-Analysen, Rentabilitätsstudien, Durchführbarkeitsstudien, Projektvorschläge, Investitionsanträge, Handlungsszenarios, Anträge zur Projektfinanzierung usw.

Initiativen zur Sensibilisierung für Informationssicherheit erfordern ein klar strukturiertes Konzept für die Erstellung des Geschäftsszenarios, das während des gesamten Projekts von der ersten Durchführbarkeitsanalyse über die Konzeption und Umsetzung bis hin zur Erreichung positiver

([20]) BERR, *2008 Information security breaches survey*, 2008, im Internet abrufbar unter http://www.security-survey.gov.uk
([21]) BERR, *2008 Information security breaches survey*, 2008, im Internet abrufbar unter http://www.security-survey.gov.uk

Ergebnisse als Orientierungshilfe dient. Ein klar strukturiertes und einheitliches Konzept für den Aufbau von Geschäftsszenarien bildet die Grundlage für ein solides Projektmanagement, von der ersten Projektbewertung bis zur erfolgreichen Durchführung.([22]) Die Geschäftsszenarien unterscheiden sich nach dem Investitionsumfang und den am Entscheidungsprozess beteiligten Führungsorganen. Die Investitionsprüfung erfolgt jedoch in der Regel nach einem ähnlichen Muster.

Die nachstehende Tabelle zeigt ein ausführliches Modell für die Erstellung eines Geschäftsszenarios, bei dem der Nutzen, die Kosten und die Gründe für die Sensibilisierungsinitiative dargestellt werden.([23]) Dieses Modell soll dazu beitragen, dass durch die Vermeidung häufiger Fehler und die Orientierung an den Ergebnissen optimale Geschäftsszenarien erstellt werden können.

Phasen	Beschreibung
Verwendung eines betriebswirtschaftlich orientierten und umfassenden Prozesses	✓ Einbeziehung aller Interessengruppen, um die Zustimmung und die kontinuierliche Unterstützung sicherzustellen. Der Erfolg der Sensibilisierungsinitiative einer Organisation hängt von der Fähigkeit der Interessengruppen ab, ein gemeinsames Ziel zu verfolgen. ✓ Im Vordergrund sollte die Frage stehen, wie die Organisation Veränderungen sowohl bei den Verfahren als auch beim Verhalten der Mitarbeiter erreichen kann. ✓ Ermittlung der möglichen Vorteile und der Personen, die sie erzielen.
Optimale Vorbereitung	✓ Um welche Chance oder welches Problem geht es? ✓ Wie stellt sich die Lage in der Organisation dar? ✓ Welche Verfahren, Produkte oder Dienstleistungen sind betroffen?
Dokumentation Ihres Verständnisses	✓ Erstellen Sie eine Beschreibung des Problems oder der Chance für Ihre Organisation. ✓ Belegen Sie, dass Sie die Verfahren, Produkte oder Dienstleistungen verstehen, die an Ihrer Initiative beteiligt oder davon betroffen sind. ✓ Stellen Sie Fragen zum Hintergrund und erörtern sie diesen. ✓ Bewerten und vertiefen Sie Ihr eigenes Verständnis. ✓ Bemühen Sie sich um Rückmeldungen, hören Sie zu und bestätigen Sie, dass Sie die Botschaft verstanden haben.
Ausführliche Dokumentation der Fallstudie	✓ Ermitteln Sie die Chancen und den Nutzen des Sensibilisierungsprogramms. ✓ Listen Sie auch sämtliche Schwachstellen, Risiken oder Bedrohungen auf, die im Rahmen der Initiative beseitigt werden könnten. ✓ Beschreiben Sie die damit verbundenen Gefahren und wie diese verringert werden können. ✓ Je sorgfältiger Sie das Geschäftsszenario erstellen, umso größer ist seine Glaubwürdigkeit.
Ermittlung des Werts für die	✓ Ermitteln Sie den Wert des Vorschlags für die Organisation. ✓ Heben Sie bei der Abwägung der technischen Details und der Auswirkungen für das Unternehmen den Wert für die Organisation

([22]) Roberts, John P., *Toolkit sample template: An effective business case,* Gartner, 11. Juli 2007; McMurchy, Neil, *Toolkit: Building the business intelligence business case — Identifying and calculating benefits,* Gartner, 25. April 2008; McMurchy, Neil, *Take these steps to develop successful bi business cases,* Gartner, 1. Februar 2008.

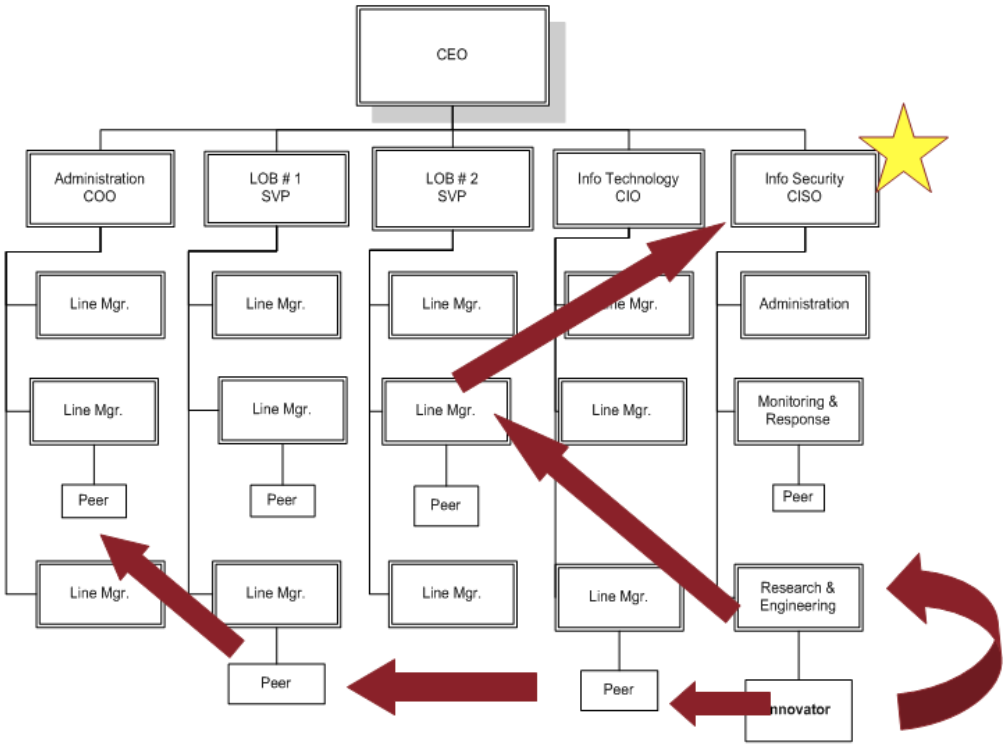
([23]) Heidt, Erik T., *Basics of the quick business case: How to champion your next information security initiative,* RSA Conference Europe 2007, 2007, im Internet abrufbar unter http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/ (zuletzt aufgerufen am 22. Juli 2008).

Organisation	und die Interessengruppen hervor. ✓ Machen Sie möglichst realistische und genaue Angaben zu den Kosten und Auswirkungen. ✓ Beschreiben Sie die Gefahren, die auftreten können, wenn diese Maßnahme nicht durchgeführt wird, und erörtern Sie Alternativen. ✓ Wecken Sie keine falschen Erwartungen!
Präsentation der Initiative	✓ Berücksichtigen Sie beim Geschäftsszenario Geschäftspläne und das Umfeld. ✓ Konzentrieren Sie sich auf die wesentlichen Elemente der Initiative und ihre Funktionsweise. ✓ Erläutern Sie Einzelheiten in Nachträgen und Anhängen, nicht in Ihrer Hauptpräsentation.

Das Geschäftsszenario kann nicht nur als Orientierungshilfe und zur Bewertung der Projektdurchführung eingesetzt werden, sondern kann auch dazu beitragen, dass der Nutzen des Projekts tatsächlich erreicht wird.

Führungsebene ansprechen

Die folgende Abbildung zeigt einen typischen Weg der Kontaktaufnahme zur Führungsebene eines Unternehmens.([24])



([24]) Heidt, Erik T., *Basics of the quick business case: How to champion your next information security initiative*, RSA Conference Europe 2007, 2007, im Internet abrufbar unter http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/ (zuletzt aufgerufen am 22. Juli 2008).

Arbeitsplan erstellen

Nachdem die Entscheidung für einen Lösungsansatz getroffen ist und das Team benannt wurde, sollte als Nächstes ein Arbeitsplan erstellt werden. In diesem Stadium enthält der Arbeitsplan zunächst nur die wichtigsten Aktivitäten mit Angabe der benötigten Ressourcen sowie der zugehörigen Zeitpläne und Eckpunkte. Wenn das eigentliche Programm erstellt wird, erfolgt eine Überprüfung des Arbeitsplans.

In einem Arbeitsplan sollten die wichtigsten Aktivitäten, Ressourcen, Zeitpläne und gegebenenfalls relevante Eckpunkte definiert werden. Mit Blick auf die effektive Abwicklung der Arbeiten wird die Verwendung einer Planungssoftware empfohlen. Anhang IV enthält ein Muster für einen Arbeitsplan.

Programm und Aufgabenkatalog ausarbeiten

Eine gute Organisation und Durchführung eines Sensibilisierungsprogramms erfordert beträchtliche Anstrengungen. Daher muss bei der Konzeption des Programms, der Weiterentwicklung der Planung bis hin zur Festlegung des Programms, der Überprüfung der bereitgestellten Ressourcen und nicht zuletzt bei der wirksamen Durchführung des Programms sehr sorgsam vorgegangen werden, damit der angestrebte Nutzen auch tatsächlich erreicht wird.

Wenn eine lange Liste von Themen zur Informationssicherheit abzuarbeiten ist, empfiehlt es sich, das Programm in getrennten Teilabschnitten zu planen, die sich über einen gewissen Zeitraum erstrecken. Auf diese Weise können Themenschwerpunkte so gesetzt werden, wie es für die jeweilige Zielgruppe sinnvoll erscheint, ohne dass sie dadurch überfordert oder weiter verunsichert wird. So sollten beispielsweise mit Blick auf die Virenproblematik alle Nutzer, die an einem Computer arbeiten, der Teil eines Netzes ist, zumindest Grundkenntnisse über Viren besitzen. In die Erklärungen zum Thema Viren können dann weitere Themenbereiche wie Konfigurationsmanagement, Netzwerk- oder Systemzugang usw. einbezogen werden.

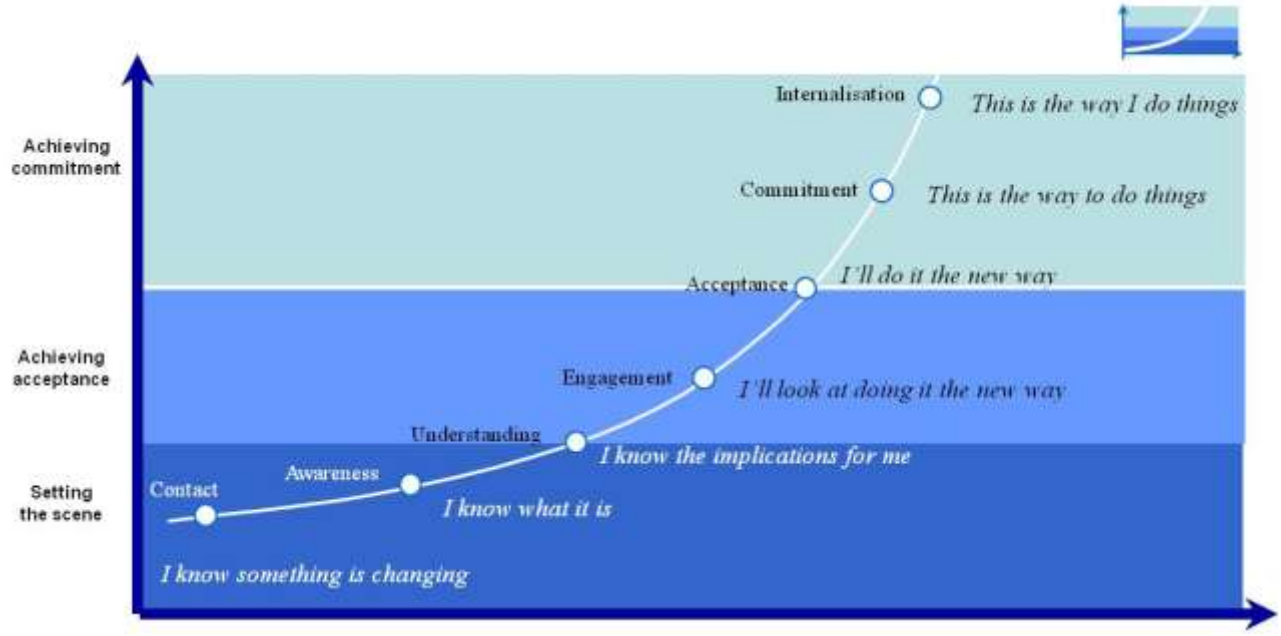
Allerdings ist es besser, auf die verwandten Themen zunächst nicht im Detail einzugehen. Hinweise, die die Zielgruppe darauf aufmerksam machen, dass verwandte Themen zu einem späteren Zeitpunkt behandelt werden, sind jedoch durchaus vertretbar. So wird bereits die Erwartung geweckt, dass im Zuge der Sensibilisierungsinitiative noch weitere sicherheitsrelevante Themen behandelt werden. Die Erwartungshaltung muss dann allerdings auch befriedigt werden, damit das Programm glaubwürdig bleibt.

Wenn die Liste der Themen, die im Rahmen des Programms behandelt werden sollen, steht, müssen die einzelnen Themen bewertet und in der Reihenfolge ihrer Priorität geordnet werden. Am einfachsten geschieht dies, indem jedem Thema ein bestimmtes Gewicht zugeordnet wird, z. B. 3 = unverzichtbar, 2 = wichtig und schließlich 1 = nützlich, aber nicht unverzichtbar. Auf diese Weise wird sichergestellt, dass die wichtigsten Themen Vorrang erhalten, sodass die Anforderungen

an das Sensibilisierungsprogramm definiert und weiter verfeinert werden können. Dies wiederum erleichtert die Ausarbeitung des zugehörigen Plans.

Kommunikationskonzept festlegen

Kommunikation ist der entscheidende Faktor für den Erfolg eines Sensibilisierungsprogramms. Eine effektive Kommunikationsplanung trägt wesentlich zum Gelingen eines Programms bei. Die nachfolgende Abbildung, in der der Zusammenhang zwischen Kommunikation und Engagement dargestellt ist, verdeutlicht, wie wichtig die Kommunikation für das Erreichen der Ziele einer Sensibilisierungsinitiative ist.



Legende

Achieving commitment	Engagement erreichen
Achieving acceptance	Akzeptanz erreichen
Setting the scene	Optimale Vorbereitung
Contact	Kontakt
Awareness	Sensibilisierung
Understanding	Verständnis
Engagement	Mitwirkung
Acceptance	Akzeptanz
Commitment	Engagement
Internalisation	Verinnerlichung
I know something is changing	Ich weiß, dass sich etwas verändert
I know what it is	Ich weiß, was sich verändert
I know the implications for me	Ich weiß, welche Auswirkungen das für mich hat
I'll look at doing it the new way	Ich werde mich bemühen, die neuen Verfahren anzuwenden
I'll do it the new way	Ich wende die neuen Verfahren an
This is the way to do things	So ist es richtig
This is the way I do things	So mach ich das immer

Wer als Manager effizient vorgehen will, setzt die notwendigen Mittel ein, um sicherzustellen, dass die erforderlichen Informationen (d. h. die Botschaft des Programms) denjenigen, die in das Programm involviert oder von dem Programm betroffen sind, zum richtigen Zeitpunkt und auf die richtige Art vermittelt werden. Für die Beteiligten oder Interessengruppen eines Programms oder einer Initiative ist es wichtig, dass die Programminformationen rechtzeitig und zielgruppengerecht formuliert zur Verfügung stehen.

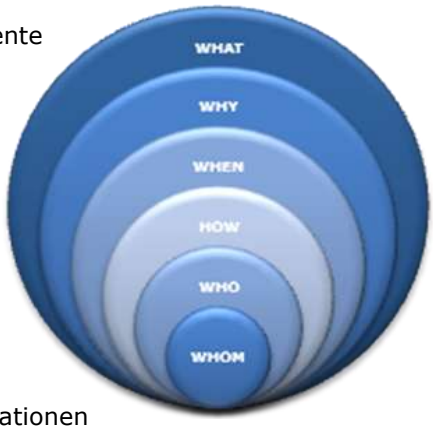
Effiziente Kommunikation

Die Auswertung zahlreicher bereits durchgeführter Sensibilisierungsinitiativen in verschiedenen Ländern ergibt eine Reihe zentraler Ansatzpunkte, die auf jede Organisation zutreffen, die beabsichtigt, eine Initiative zur Sensibilisierung für Informationssicherheit durchzuführen.

Nachstehend einige Empfehlungen für eine wirkungsvolle Kampagne.

Grundlagen

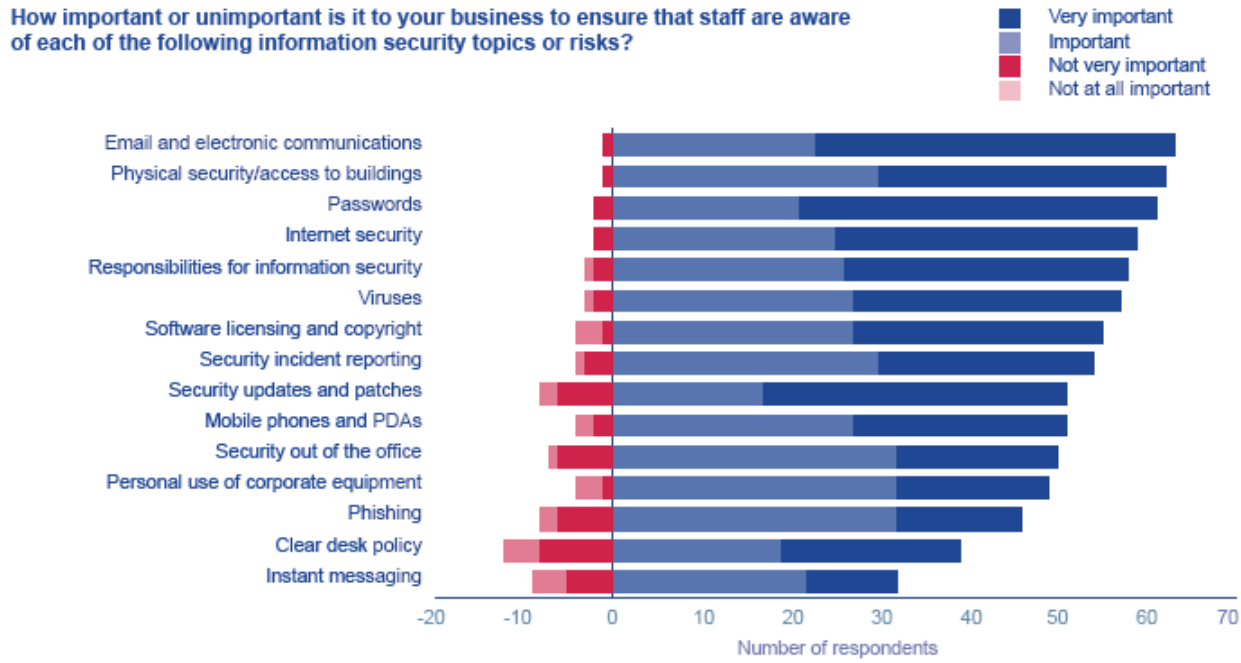
- ✓ Ein möglichst breites Zielpublikum ansprechen. Es empfiehlt sich, Multiplikatoreneffekte zu nutzen, um eine möglichst große Reichweite der Botschaft zu erzielen.
- ✓ Die Situation nicht dramatisieren oder übertrieben negativ darstellen. Wenn näher auf Problemfelder oder Risiken eingegangen werden muss, sind Beispiele aus der eigenen Erfahrungswelt für das Zielpublikum meist leichter zu verstehen.
- ✓ Ziel jeder Sensibilisierungsinitiative muss es sein, bei der Zielgruppe eine positive Veränderung ihres Sicherheitsverhaltens herbeizuführen.
- ✓ Die Botschaft, die vermittelt wird, die Kommunikationskanäle und der Absender der Botschaft müssen einflussreich und glaubhaft sein, sonst kommt die Botschaft bei der Zielgruppe nicht an.
- ✓ Die Zielgruppe bezieht ihre Informationen aus unterschiedlichen Quellen. Um sie erfolgreich anzusprechen, müssen verschiedene Kommunikationskanäle genutzt werden.
- ✓ Die Initiative sollte möglichst flexibel und anpassungsfähig sein, da nicht selten das Umfeld durch externe Faktoren verändert wird.
- ✓ Jede wesentliche Kommunikation sollte folgende Elemente beinhalten:([25])
  - WAS wird von der Zielgruppe erwartet, die die Information erhält?
  - WARUM sollte das Zielpublikum an dem Sensibilisierungsprogramm teilnehmen und worin besteht der Nutzen?
  - WANN sollte der Empfänger die verlangten Maßnahmen durchführen?
  - WIE hängen die Maßnahmen mit den Verantwortlichkeiten und der Leistung der Zielgruppe bei ihrer Arbeit und/oder mit ihrem Leben zusammen?
  - WER ist Träger des Programms?
  - WEN sollte man ansprechen, wenn weitere Informationen benötigt werden?



([25]) Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

Themen

Die Ermittlung der für die Organisation und das Zielpublikum wesentlichen Themen im Bereich der Informationssicherheit ist der erste der zahlreichen Schritte, die zur Organisation einer Sensibilisierungsinitiative erforderlich sind. Eine kürzlich veröffentlichte Publikation der ENISA belegt, dass E-Mail und elektronische Kommunikation, Passwörter, Sicherheits-Updates und -Patches für die Unternehmen eine sehr wichtige Rolle spielen. Als weitere wichtige Elemente werden unter anderem auch das Berichtswesen für Sicherheitsvorfälle, der private Gebrauch von Unternehmensausrüstung und die Sicherheit außerhalb des Arbeitsplatzes genannt.([26]) Die nachstehende Grafik vermittelt einen umfassenderen Überblick über die in dieser Publikation enthaltenen Daten.



Legende

How important or unimportant is it to your business …	Wie wichtig oder unwichtig ist es für Ihr Unternehmen, dass alle Mitarbeiter über alle der folgenden Aspekte oder Risiken in Bezug auf die Informationssicherheit informiert sind?
Very important	Sehr wichtig
Important	Wichtig
Not very important	Nicht sehr wichtig
Not at all important	Überhaupt nicht wichtig
Email and electronic communications	E-Mail und elektronische Kommunikation
Physical security/access to buildings	Physische Sicherheit/Zugang zu Gebäuden
Passwords	Passwörter
Internet security	Internetsicherheit

([26]) ENISA, *Sensibilisierungsmaßnahmen zur Informationssicherheit: Die übliche Praxis und die Erfolgsmessung*, 2007, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/kpi/measuring_aw_de.pdf

Responsibilities for information security	Verantwortlichkeiten für Informationssicherheit
Viruses	Viren
Software licensing and copyright	Softwarelizenzen und Urheberrechte
Security incident reporting	Berichtswesen für Sicherheitsvorfälle
Security updates and patches	Sicherheits-Updates und –Patches
Mobile phones and PDAs	Mobiltelefone und PDAs
Security out of the office	Sicherheit außerhalb des Arbeitsplatzes
Personal use of corporate equipment	Privater Gebrauch von Unternehmensausrüstung
Phishing	Phishing
Clear desk policy	„Clear-Desk-Policy"
Instant messaging	Instant Messaging
Number of respondents	Anzahl der Befragten

Die folgende Aufzählung relevanter Themen für die Sensibilisierung im Bereich der Informationssicherheit ist nicht vollständig und sollte lediglich aus Ausgangsbasis zur Ermittlung der Themen für Ihr Sensibilisierungsprogramm betrachtet werden:

- ✓ Grundsätze und Strategien der Informationssicherheit
- ✓ Sicherheit am Bildschirmarbeitsplatz
- ✓ Strategien für den Umgang mit Websites
- ✓ E-Mail-Sicherheit
- ✓ Social Engineering
- ✓ Sicherheit bei Dritten und Partnern
- ✓ Identitätsprüfung
- ✓ technische Sicherheitsmechanismen
- ✓ Einstufung und Kontrolle von Informationen
- ✓ Reaktion auf Sicherheitsvorfälle
- ✓ Sachmittelverwaltung (z. B. von USB-Speichersticks, Druckern, PDAs, Mobiltelefonen)
- ✓ usw.

Wenn die Themen festgelegt sind, ist es sinnvoll, die Zielgruppen den entsprechenden Themen zuzuordnen. Anhand dieser einfachen Zuordnung der Zielgruppen können die Inhalte der Schulungen festgelegt werden, die für die jeweiligen Rollen durchgeführt werden sollen.

Mit der einfachen Zuordnung der Themen zu Funktionen und Zielgruppen können die Inhalte der Schulungen festgelegt werden, die für die jeweiligen Rollen durchgeführt werden sollen. Anhang V enthält ein Muster für die Zuordnung der Themen zu den Rollen.

Botschaft

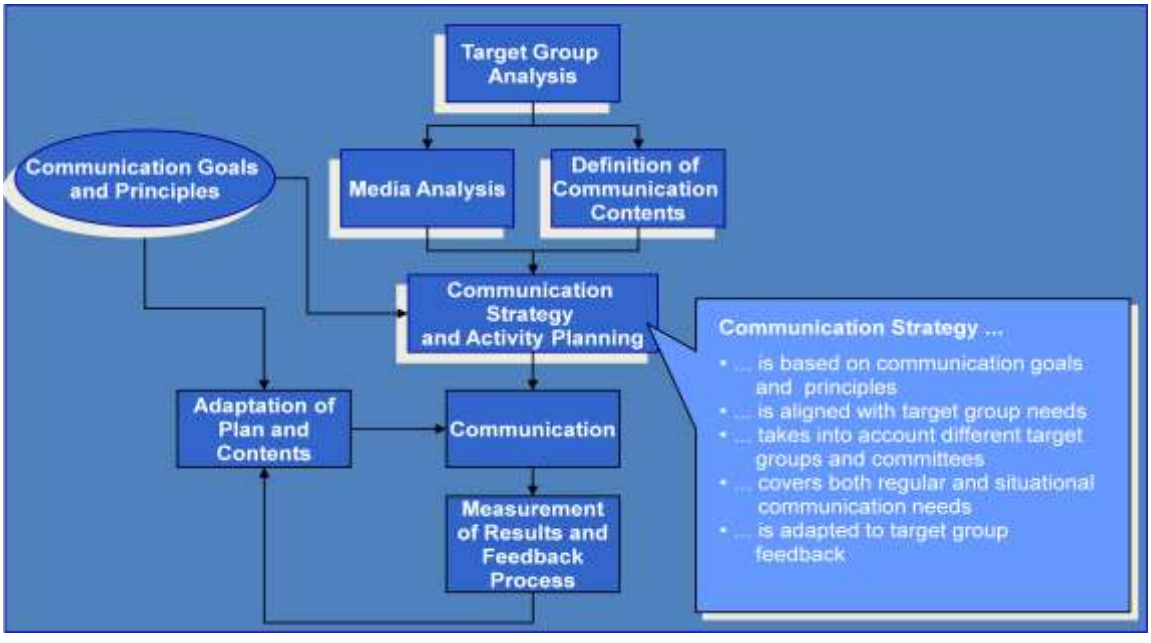
- ✓ Ziel ist, über die wirksamsten Kommunikationskanäle die richtige Botschaft dem richtigen Zielpublikum zu vermitteln. Auf diese Weise wird die Überzeugungskraft der Botschaft

optimiert und das Zielpublikum zum Handeln veranlasst – insbesondere dann, wenn die Botschaft die Interessen und Bedürfnisse der Zielgruppe anspricht. Die Botschaft kann und sollte gezielt auf den Kenntnisstand oder die technischen Fähigkeiten der Zielgruppe ausgerichtet sein. Für die Konzeption einer wirksamen Kampagne sollten im Vorfeld entsprechende Informationen gesammelt werden.

- ✓ Die Botschaft muss proaktiv, zielgruppengerecht und einheitlich formuliert werden. Eine Liste mit „10 wichtigen Tipps" ist ein gutes Mittel – sie ist kurz und knapp in der Darstellung und damit leicht verständlich und schnell zur Hand.
- ✓ Kurz gesagt sollte eine Botschaft als Teil einer Sensibilisierungsinitiative Risiken und Gefahren nennen, denen die Nutzer ausgesetzt sind; sie sollte aussagen, weshalb dies für die Nutzer relevant ist, was sie tun und was sie lassen sollen und nicht zuletzt, wie sie sich schützen können.
- ✓ Die Botschaft muss die Zielgruppe ansprechen. Die Zielgruppe wird tagtäglich von einem riesigen Informationsangebot überflutet, deshalb kommt es darauf an, kreative Mittel und Wege zu finden, um die Botschaft so zu übermitteln, dass sie wahrgenommen wird. Hilfreich sind hier zentrale durchgängig verwendete Themen und/oder Slogans.

Mehrwert

- ✓ Der Zielgruppe sollte – soweit dies machbar ist – die Möglichkeit gegeben werden, ein Feedback zu der Kampagne zu geben; dies hilft bei der weiteren Verbesserung der Kampagne oder nachfolgender Initiativen.
- ✓ Planung und Durchführung einer Kampagne sind nur die eine Hälfte der Arbeit. Anschließend sollte auch eine Evaluierung (anhand von Messgrößen, Leistungszielen usw.) vorgenommen werden, um die Wirksamkeit der Kampagne zu ermitteln und Erfahrungswerte für die Gestaltung zukünftiger Initiativen zu gewinnen. Als Erfolgsindikator können Messgrößen wie die Zahl der Besucher einer Website, die Zahl der Downloads oder angeforderten Publikationen oder die Zahl der veröffentlichten Zeitungsartikel dienen.
- ✓ Anhand qualitativer (z. B. Fokusgruppen, Umfragen) und/oder quantitativer Erhebungen (z. B. Fragebogen, Mehrthemenbefragungen) lässt sich eine Evaluierung der Wirksamkeit verschiedener auf die Zielgruppe ausgerichteter Sensibilisierungskampagnen vornehmen. Siehe hierzu das Kapitel über die Programmevaluierung.
- ✓ Beispiele für bewährte Verfahren und spezifische Sensibilisierungsinitiativen lassen sich auch bei anderen Organisationen mit vergleichbarer Nutzerstruktur finden.
- ✓ Eine Kommunikationsstrategie ist ein zentrales Element bei allen Sensibilisierungsmaßnahmen, sie muss jedoch an die Bedürfnisse und den spezifischen Kontext angepasst werden.



Legende

Target group analysis	Zielgruppenanalyse
Communication goals and principles	Kommunikationsziele und -grundlagen
Media Analysis	Medienanalyse
Definition of Communication Contents	Festlegung der Kommunikationsinhalte
Communication Strategy and Activity Planning	Kommunikationsstrategie und Arbeitsplanung
Communication Strategy … … is based on communication goals and principles … is aligned with target group needs … takes into account different target groups and committees … covers both regular and situational communication needs … is adapted to target group feedback	Kommunikationsstrategie … … basiert auf Kommunikationszielen und -grundlagen … wird auf die Bedürfnisse der Zielgruppen abgestimmt … berücksichtigt unterschiedliche Zielgruppen und Ausschüsse … deckt sowohl den regelmäßigen als auch den situationsbezogenen Kommunikationsbedarf ab … wird entsprechend dem Feedback der Zielgruppe angepasst
Adaption of Plan and Contents	Anpassung von Plan und Inhalten
Communication	Kommunikation
Measurement of Results and Feedback Process	Messung der Ergebnisse und Feedback-Mechanismus

Anhand der wichtigen Einzelschritte im Prozessablauf einer effektiven Sensibilisierungs- und Schulungsinitiative lässt sich eine Strategie aufstellen.

Prozess	Beschreibung
Ziele und Zielvorgaben der Initiative festlegen/ Zielgruppen bestimmen	• Fragen Sie nach, weshalb die Kampagne durchgeführt werden soll, welches die zentralen Themen sein sollen, weshalb diese Themen aufgegriffen werden sollen und ob dies die geeignete Organisation hierfür ist. • Verlassen Sie sich nicht auf Annahmen – soweit möglich, Daten beschaffen und Methoden, wie z. B. Fokusgruppen, nutzen. • Legen Sie Messgrößen für die Leistungsmessung der Kampagne und als Hilfe für die Ermittlung von Erfahrungswerten fest.
Gegebenenfalls Partner suchen	• Suchen Sie sich eine andere Organisation als Partner, wenn Sie keinen Zugang zum vorgesehenen Zielpublikum bekommen, wenn Ressourcen fehlen oder Ihr Zielpublikum beim Thema Informationssicherheit einer anderen Organisation mehr vertraut. • Die Partner müssen die gleiche Botschaft vermitteln und eine einheitliche Meinung vertreten.
Botschaft auf eine bestimmte Zielgruppe ausrichten	• Die angesprochene Zielgruppe muss möglichst homogene Interessen und Prioritäten haben; in der allgemeinen Öffentlichkeit sind Interessen, Kenntnisse und Erfahrungen zu unterschiedlich. Weil unterschiedliche Adressaten auf unterschiedliche Risiken ansprechen (oft aufgrund persönlicher Erfahrungen), muss die Botschaft auf eine bestimmte Zielgruppe ausgerichtet sein. • Fragen Sie nach, was bei den Adressaten ankommt oder ihre Aufmerksamkeit weckt, weshalb ihnen das Thema wichtig sein sollte (auf ihre Belange und Bedürfnisse zugeschnitten) und wie sie sich verhalten werden.
Botschaft ausgestalten	• Stellen Sie sich auf die Adressaten ein: Inwieweit sind sie sich der Problematik bewusst, welche Bedürfnisse haben sie, worüber machen sie sich Sorgen, woher beziehen sie ihre Informationen und welche Informationen erwarten sie? • Die eigentliche Botschaft muss dreierlei bewirken: die Aufmerksamkeit der

	Adressaten wecken, sie für die Gefahren sensibilisieren und ihnen Informationen vermitteln oder aufzeigen, woher sie Informationen bekommen. • Die Botschaft darf möglichst nicht ausgrenzen – keine Diskriminierung von Minderheiten usw.
Botschaft testen	• Starten Sie die Kampagne und werten Sie die Ergebnisse bzw. Reaktionen aus. Eine (quantitative und qualitative) Evaluierung kann u. a. anhand von Fokusgruppen, persönlichen Befragungen, Fragebogen oder Mehrthemenbefragungen durchgeführt werden.

Am effizientesten lässt sich die Botschaft einer Sensibilisierungs- und Schulungsinitiative mithilfe von Multiplikatoren vermitteln. Sie verbreiten die Botschaft an einen möglichst großen Adressatenkreis innerhalb der Zielgruppe.

Für die Weitergabe von Botschaften im Rahmen einer Initiative kommen verschiedene Partner oder Multiplikatoren infrage, so zum Beispiel:

- ✓ Erwachsenenbildungsprogramme
- ✓ Banken
- ✓ Unternehmen
- ✓ Bürgerzentren
- ✓ Bildungseinrichtungen
- ✓ Computerläden
- ✓ unabhängige Einrichtungen
- ✓ Branchenorganisationen (Gewerkschaften, Verbände)
- ✓ Institutionen
- ✓ Internetdiensteanbieter
- ✓ bekannte Fachleute
- ✓ Bibliotheken
- ✓ örtliche Handelsverbände
- ✓ Medien
- ✓ NRO
- ✓ Eltern-Lehrer-Verbände
- ✓ Hochschulen
- ✓

Kommunikationskanäle

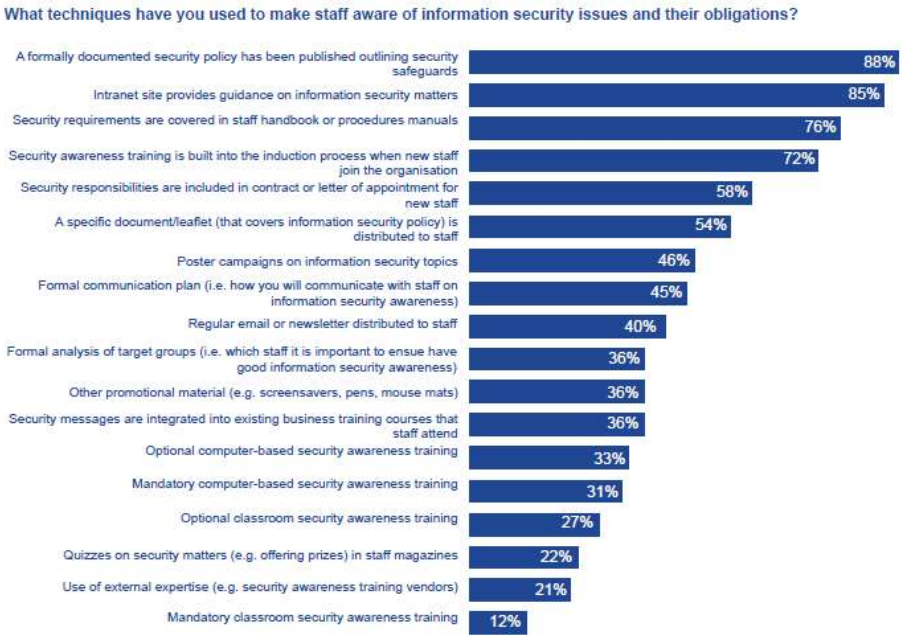
In der nachfolgenden Übersicht sind einige der Hauptkommunikationskanäle aufgeführt, die für die Sensibilisierung im Rahmen einer Initiative zur Informationssicherheit genutzt werden können. In der Übersicht werden nur einige der jeweiligen Vor- und Nachteile der verschiedenen Kanäle genannt, sie ist keinesfalls als umfassende Aufstellung zu verstehen.

Kanal	*Vorteile*	*Nachteile*
Broschüre oder Magazin	✓ Inhalt und Format der Botschaft können problemlos definiert werden. ✓ Die Zielgruppe kann sich eingehend mit dem Inhalt befassen. ✓ Festgelegte Adressaten können erreicht werden.	× Keine absolut verlässliche/dauerhafte Informationsquelle, da Informationsmaterial verloren gehen kann. × Spricht möglicherweise nur eine bestimmte Zielgruppe an.
Comic	✓ Spricht bestimmte Zielgruppen (z. B. Jugendliche) unmittelbar an.	× Wiedergabe von detaillierteren Botschaften ist schwierig.

	✓ Auch eher abstrakte Inhalte lassen sich vermitteln.	× Spricht möglicherweise nur eine bestimmte Zielgruppe an.
Fernlernen — Computerunterstützte Schulung (CBT) — Online-Schulung	✓ Ermöglicht Schulung auch in unterschiedlichen geografischen Gebieten. ✓ Detailliertere Inhalte können vermittelt werden.	× Erstellung von Schulungsprogrammen ist u. U. kostenintensiv. × Setzt technisches Vorwissen der Teilnehmer voraus.
Bildungswesen — Unterrichtspaket — Lehrmaterial	✓ Gute Möglichkeit, eine große Zahl von Schülern zu erreichen. ✓ Häufig können bestehende Kanäle genutzt werden.	× An den Schulen ist die Zeit knapp, die Lehrpläne sind oft ohnehin bereits überfrachtet. × Den Lehrern fehlt u. U. das erforderliche Fachwissen für die Übermittlung der Botschaft. × An den Schulcomputern sind manche Aktivitäten u. U. nicht möglich, z. B. Üben der Installation von Antiviren-Programmen.
E-Mail	✓ Relativ preisgünstiger Kanal, um einen großen Adressatenkreis anzusprechen. ✓ Die Zielgruppe kann sich mit den Informationen befassen, wenn sie Zeit hat.	× Die Botschaft geht u. U. in der Masse der E-Mails und Spam-Mails unter. × E-Mail-Adressen müssen bekannt sein.
Veranstaltung — Messe — Tagung — Seminar — Konferenz	✓ Durch gezielte Auswahl von Themen und Veranstaltungsorten lässt sich ein breites Zielpublikum erreichen. ✓ Aufgrund der interaktiven Komponente bestehen gute Chancen, das Publikum für das Thema zu interessieren.	× Möglicherweise wird die Veranstaltung von der Zielgruppe gar nicht besucht. × Kein proaktiver Kanal – Teilnahme der Zielgruppe erforderlich.
Flyer oder Info-Blatt	✓ Bietet Gelegenheit, viel Information zu vermitteln. ✓ Kostengünstig in der Herstellung.	× Erfordert Organisation von Vertriebskanälen, damit das gewünschte Zielpublikum erreicht wird. × Keine absolut verlässliche/dauerhafte Informationsquelle, da Informationsmaterial verloren gehen kann.
Elektronischer Newsletter	✓ Ähnliche Vorteile wie E-Mail.	× Kein proaktiver Kanal, da sich die Nutzer in der Regel erst registrieren lassen müssen. × Setzt technisches Vorwissen der Nutzer voraus.
Tageszeitung	✓ Großauflage mit tiefer Marktdurchdringung. Gemessen an den Stückkosten sind Zeitungen ein kostengünstiges Medium, um mit einer Botschaft ein großes Publikum zu erreichen. ✓ In eine Zeitungsanzeige kann der Detaillierungsgrad der Informationen nach Bedarf bestimmt werden, außerdem Möglichkeit zur Wiedergabe von Bildern und Logos.	× Der „Überflutungsfaktor": In der Zeitung wetteifern zahlreiche Informationen um die Aufmerksamkeit des Lesers. Meist sehr viele Anzeigen in unterschiedlicher Größe und Gestaltung für eine Vielzahl von Produkten und Dienstleistungen. × Wenn nur ein bestimmtes Segment der Bevölkerung angesprochen werden soll, u. U. zu große

		Streubreite. × Kurzlebiges Medium. Wird häufig nur kurz überflogen, nicht intensiv gelesen.
Telefon	✓ Direkte Ansprache der Zielgruppe. ✓ Durch die interaktive Komponente gute Chance, die Zielgruppe für das Thema zu interessieren.	× Kann relativ teuer werden. × Telefonnummern der Zielgruppe müssen bekannt sein.
Plakat	✓ Kann durch Größe und Format Aufmerksamkeit wecken. ✓ Durch umfangreiche Plakatierung Informationen für jedermann zugänglich.	× Gefahr, dass die Botschaft in der Fülle an Informationsmaterial untergeht.
Rundfunk	✓ Größter Vorteil ist die hohe Wiederholrate (Frequenz) (Zielpublikum wird wiederholt angesprochen) bei vertretbaren Kosten. ✓ Sendeformate helfen dabei, Interessengruppen und bestimmte Bevölkerungsgruppen gezielt anzusprechen.	× Stark kommerzialisiertes Medium. × Keine Möglichkeit zur visuellen Präsentation bzw. Demonstration. × Ein Radiospot ist nicht so dauerhaft wie die gedruckte Botschaft. × Aufgrund von Sendeformaten und Spezialisierung auf ein bestimmtes Publikum lässt sich über einen einzigen Sender meist kein breites Publikum ansprechen.
Bildschirmschoner	✓ Die Information erscheint auf dem Bildschirm und wird von den Nutzern wahrgenommen.	× Erfordert Entwicklungsaufwand. × Installation erfordert gewisse Vorkenntnisse. × Nutzer ohne eigenen Computer werden nicht erreicht.
SMS	✓ Die Zielgruppe wird direkt angesprochen.	× Erfordert Zusammenarbeit mit Telekommunikationsanbieter. × Effektiver Kanal, um die Zielgruppe auf Gefahren aufmerksam zu machen, aufgrund der Textlängenbegrenzung jedoch kein Medium zur Sensibilisierung.
Schulung	✓ Bietet durch die interaktive Komponente die Möglichkeit, das Zielpublikum direkt anzusprechen und für das Thema zu interessieren. ✓ Inhalt der Botschaft kann mehr ins Detail gehen und an die Zielgruppe angepasst werden.	× Kein proaktiver Kanal – Teilnahme der Zielgruppe erforderlich. × Erfordert gewisse Ressourcen und logistischen Aufwand, daher ungeeignet, um ein Massenpublikum zu erreichen.
Fernsehen	✓ Hoher Wirkungsgrad, Kombination von Bild, Ton und Bewegung – weckt Aufmerksamkeit, Erinnerungseffekt. ✓ Fernsehen kommt der unmittelbaren Kommunikation so nahe wie kein anderes Medium. ✓ Persönliche Botschaft einer Autoritätsperson kann sehr überzeugend wirken. ✓ Die Botschaft kann demonstriert werden. ✓ Gezielte Publikumsansprache durch	× Kosten – setzt ein relativ hohes Budget voraus. × Sendeplatz kann zwar frei gewählt werden, besonders publikumswirksame Sendeplätze sind jedoch möglicherweise bereits vergeben.

	Programmwahl. Zeitliche Flexibilität durch unterschiedliche Sendeplätze zu verschiedenen Tageszeiten. Möglichkeit, auf große Reichweite oder hohe Frequenz abzustellen.	
Video — DVD — CD	✓ Bietet große Gestaltungsfreiheit. ✓ Bei fachgerechter Umsetzung wird die Botschaft durch professionelle Wiedergabe verstärkt.	× Mit neueren Technologien wenig vertrautes Publikum wird u. U. nicht erreicht.
Website	✓ Kann nach Bedarf aktualisiert werden. ✓ Möglichkeit zur Präsentation von Inhalten für unterschiedliche Zielgruppen. ✓ Problemlose Weiterleitung zu weiterführenden Informationen.	× Mit neueren Technologien wenig vertrautes Publikum wird u. U. nicht erreicht. × Setzt technisches Vorwissen voraus. × Kein proaktiver Kanal – aufgrund der Vielzahl an Websites und der Informationsflut im Internet wird die Botschaft möglicherweise übersehen.



Eine unlängst von der ENISA durchgeführte Umfrage ergab, dass unter den gängigen Verfahren, mit denen Mitarbeiter auf ihre Pflichten in Sicherheitsbelangen aufmerksam gemacht werden, formal dokumentierte Sicherheitsvorschriften, Handbücher für Mitarbeiter, Einführungsprogramme sowie Präsenzschulungen die gebräuchlichsten Verfahren sind.([27]) Diese Tendenz wird durch die Zahlen der BERR-Erhebung 2008 bestätigt, der zufolge es in 88 % der großen Unternehmen im Vereinigten Königreich formal dokumentierte und festgelegte Sicherheitsvorschriften gibt. 54 % aller britischen Unternehmen machen ihre Mitarbeiter in einem speziellen Mitarbeiterhandbuch auf ihre Pflichten in Sicherheitsbelangen aufmerksam, 40 % durch Präsenzschulungen und Präsentationen und 39 % beim Eintritt in das Unternehmen oder in einem Einführungsprogramm.([28])

([27]) ENISA, *Sensibilisierungsmaßnahmen zur Informationssicherheit: Die übliche Praxis und die Erfolgsmessung*, 2007, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/kpi/measuring_aw_de.pdf

([28]) BERR, *2008 Information security breaches survey*, 2008, im Internet abrufbar unter http://www.security-survey.gov.uk

Legende

What techniques have …	Welche Methoden haben Sie eingesetzt, um Ihre Mitarbeiter für Informationssicherheitsthemen zu sensibilisieren und auf ihre Pflichten aufmerksam zu machen?
A formally documented …	Es wurden formal dokumentierte Sicherheitsvorschriften veröffentlicht, in denen Schutzmaßnahmen dargelegt werden
Intranet site provides …	Eine Intranetseite bietet die Möglichkeit, sich über Informationssicherheit zu informieren
Security requirements …	Sicherheitsanforderungen sind in einem Handbuch für Mitarbeiter oder Verfahrenshandbuch dokumentiert
Security awareness is built …	Die Sensibilisierung für Sicherheitsbelange ist Teil des Einführungsprozesses für neue Mitarbeiter
Security responsibilities are …	Die Verantwortung für Sicherheitsbelange ist im Einstellungsvertrag für neue Mitarbeiter verankert
A specific document/leaflet …	Die Mitarbeiter erhalten ein spezielles Dokument/Broschüre (zu den Vorschriften für Informationssicherheit)
Poster campaigns …	Plakatkampagnen zu Informationssicherheitsthemen
Formal communication plan …	Formaler Kommunikationsplan (in dem festgelegt ist, wie die Kommunikation mit den Mitarbeitern zur Sensibilisierung für Informationssicherheit erfolgt)
Regular e-mail or newsletter …	Regelmäßiger Versand von E-Mails oder Newslettern an die Mitarbeiter
Formal analysis of target groups …	Formale Analyse der Zielgruppen (d. h., bei welchen Mitarbeitern ist es besonders wichtig, dass sie für Fragen der Informationssicherheit sensibilisiert sind?)
Other promotional material …	Weitere Werbematerialien (z. B. Bildschirmschoner, Kugelschreiber, Mousepads)
Security messages are integrated …	Sicherheitsbotschaften werden in bestehende Schulungslehrgänge für die Mitarbeiter integriert
Optional computer-based …	Optionale computerunterstützte Schulungsmaßnahmen
Mandatory computer-based …	Obligatorische computerunterstützte Schulungen zur Sicherheitssensibilisierung
Optional classroom …	Optionale Präsenzschulungen zur Sicherheitssensibilisierung
Quizzes on security …	Quizspiele zu Sicherheitsthemen in Mitarbeiterzeitschriften (z. B. Preisausschreiben)
Use of external expertise …	Einsatz von externen Fachleuten (z. B. Drittanbieter von Schulungen zur Sicherheitssensibilisierung)
Mandatory classroom …	Obligatorische Präsenzschulungen zur Sicherheitssensibilisierung

Leitfaden für die Kommunikationsplanung

In diesem Kapitel wird ein Konzept mit dem zugehörigen Prozess für die Entwicklung eines umfassenden Kommunikationsplans durch eine Organisation beschrieben. Die vorgestellten Vorlagen und Hilfsmittel können den mit der Durchführung von Sensibilisierungskampagnen betrauten Teams als Grundlage dienen.

Der Prozess

Die Ausarbeitung eines konkreten Kommunikationsplans entscheidet mit darüber, ob es gelingt, die gewünschte Verhaltensänderung der Zielgruppe herbeizuführen. Wir empfehlen hierfür eine in fünf Schritte untergliederte Vorgehensweise:

Die wichtigsten Merkmale des Prozesses

- ✓ Die Wahl der Kommunikationsaktivitäten wird durch die Kommunikationsziele vorgegeben.
- ✓ Die Zielgruppenanalyse hilft bei der Bestimmung der wichtigen Zielinteressengruppen und der Benennung von Zielvorgaben und Anforderungen.
- ✓ Die zentralen Botschaften müssen speziell auf die Thematik abgestimmt und auf die einzelnen Zielgruppen ausgerichtet sein.
- ✓ Im Kommunikationsplan werden Botschaft, Medien und Frequenz der Kommunikation für die jeweilige Zielgruppe definiert. Das Timing der einzelnen Botschaften wird so gewählt, dass es mit dazu beiträgt, die Meilensteine des Sensibilisierungsprogramms zu erreichen.
- ✓ Das Feedback der Zielgruppe ist ausschlaggebend für die Sicherung von Qualität, Konsistenz und Effektivität der Kommunikation.

Kommunikationsziele

Bei der Kommunikation zum Thema Informationssicherheit geht es darum, den Erfolg der Sensibilisierungsinitiative dadurch zu unterstützen, dass alle wichtigen Zielgruppen wirksam angesprochen, eingebunden und motiviert werden. Als mögliche Kommunikationsziele kommen infrage:

- ✓ Die strategische Vision für Netz- und Informationssicherheit und ihren Nutzen in der breiten Öffentlichkeit bekannt zu machen;
- ✓ alle identifizierten Zielgruppen anzusprechen und aktiv einzubinden;
- ✓ die betroffenen Zielgruppen mit dem Thema Informationssicherheit und seiner Bedeutung für sie selbst vertraut zu machen;
- ✓ den Angehörigen der Zielgruppe Gelegenheit zu bieten, Fragen zu stellen und Probleme zu besprechen;
- ✓ Energie aufzubauen und Impulse zu entwickeln, die das Entstehen eines neuen lernenden Umfelds fördern.

Zielgruppenanalyse vornehmen und Kommunikationskanal bestimmen

Die verschiedenen Zielgruppen zu bestimmen und sie richtig einzubinden, ist erfolgsentscheidend.

Eine Gesellschaft besteht aus einer Vielzahl von Individuen mit unterschiedlichen Interessen, Kenntnissen und Prioritäten. Das macht es schwierig, Themen und Botschaften zu finden, die alle ansprechen. In aller Regel ist es daher erforderlich, spezifische Zielgruppen mit vergleichbaren Interessen und Prioritäten zu bestimmen. Nachdem die einzelnen Zielgruppen vom

Sensibilisierungsteam festgelegt wurden, müssen für jede dieser Gruppen folgende Faktoren bestimmt werden:

- ✓ Inwieweit ist sich die Zielgruppe des Themas Informationssicherheit bewusst?
- ✓ Inwieweit ist sie bereits mit entsprechenden Lösungskonzepten vertraut?
- ✓ Für welche Zwecke werden IKT genutzt?
- ✓ Welches sind für die Zielgruppe die wichtigsten Probleme?
- ✓ Woher bezieht die Zielgruppe bislang ihre Informationen?

Bei der inhaltlichen Festlegung der Sensibilisierungsinitiative sollten Erfahrung und Vorwissen der Zielgruppen berücksichtigt werden. Nachstehend werden die Schritte zur Durchführung einer Zielgruppenanalyse anhand eines Beispiels veranschaulicht.

Schritte zur Durchführung einer Zielgruppenanalyse – Beispiel

Zielgruppen bestimmen	Zielgruppen sind diejenigen Gruppen, die durch den Grad der Sensibilisierung für das Thema Informationssicherheit beeinflusst werden oder die ihrerseits das Bewusstsein für das Thema beeinflussen können.
Die Sachlage erkennen	Die Zielgruppe ist u. U. besorgt wegen der Folgen für ihre Organisation, Kontrollverlust usw.
Den Grad der Sensibilisierung bewerten	Der Sensibilisierungsgrad der einzelnen Zielgruppen für Fragen der Informationssicherheit und ihre Kenntnisse von Lösungskonzepten werden bewertet: H (hoch), M (mittel), G (gering).
Erwünschtes Verhalten bestimmen	Festlegen, welches Verhalten die einzelnen Zielgruppen an den Tag legen müssen, damit die wichtigsten Probleme angegangen werden.

Vorteile einer genauen Zielgruppenanalyse

- ✓ Informations- und Handlungsbedarf lassen sich genauer eingrenzen.
- ✓ Es wird deutlich herausgearbeitet, welche Auswirkungen Probleme im Bereich Informationssicherheit haben und mit welchen Maßnahmen sich diese Probleme beheben lassen.
- ✓ Bei der Ausarbeitung des Kommunikationsplans kann gezielt darauf geachtet werden, dass den Angehörigen der Zielgruppe zum richtigen Zeitpunkt auf dem richtigen Wege die richtigen Informationen vermittelt werden.
- ✓ Das Sensibilisierungsteam kann bewusst und gezielt auf den Sensibilisierungsgrad der einzelnen Zielgruppen eingehen.

Nach erfolgter Zielgruppenanalyse können angemessene Kommunikationsziele festgelegt und geeignete Kommunikationskanäle bestimmt werden. Die nachstehende Matrix veranschaulicht eine mögliche Vorgehensweise.

Kommunikationsziele (*)

Zielgruppe	Sensibilisieren	Problembewusstsein schaffen	Kenntnisse aufbauen	Lösungen vermitteln
Gruppe 1		√	√	√
Gruppe 2	√	√	√	√
Gruppe 3	√	√		

Gruppe 4	√	√	√	√
Gruppe 5	√	√		

(*) Beispiele für Ziele und Kanäle	Website E-Mail Newsletter Publikationen	Präsentationen Tagungen Konferenzen	Workshops Fragestunden	Workshops Seminare Memos

Geeignete Kommunikationskanäle (*)

Zentrale Botschaften bestimmen

Zwischen Botschaft und Zielgruppe besteht ein enger Zusammenhang mit wechselseitiger Einflussnahme. So kann beispielsweise die Botschaft auf den Umgang mit einer bestimmten Kategorie von Risiken (z. B. Bedrohung der Privatsphäre) oder auf eine bestimmte Technologie (z. B. Mobiltelefone) ausgerichtet werden. Ein Zielpublikum, das bislang noch wenig Erfahrung mit dem Thema Informationssicherheit hat, wird am ehesten eine Botschaft zur Kenntnis nehmen und verstehen, die sich darauf bezieht, wie es selbst IKT nutzt oder wie es mit IKT interagiert. Beispiel: „Wenn Sie mit dem Handy telefonieren, müssen Sie Folgendes beachten ...". Eine solche Botschaft wird eher verstanden als eine allgemeine Aussage zum Thema „Schutz der Privatsphäre". Wie nachstehend gezeigt, kann eine Botschaft auch mehrere Zielgruppen ansprechen.

Beispiele für zentrale Botschaften	Zielgruppe 1	Zielgruppe 2	Zielgruppe 3	Zielgruppe 4	Zielgruppe 5	Zielgruppe 6	Zielgruppe 7
Hinweis auf die Wichtigkeit von Sicherungskopien	√	√	√	√	√	√	√
Schutz personenbezogener Daten im Internet (Online-Shopping, -Banking, -Abstimmung, usw.)	√	√	√	√	√	√	√
Kinder mit dem Internet vertraut machen, damit sie es gezielt nutzen können	√			√	√		
Für Bluetooth-Hacker unerkennbar bleiben	√	√		√	√		
...	√	√				√	√
...	√	√		√	√		
...	√	√		√	√		

Beispiel

Rollen und Verantwortungsbereiche zuweisen

Jedes Mitglied des Sensibilisierungsteams (einschließlich etwaiger Partner) übernimmt in der Kommunikation eine bestimmte Rolle bzw. operiert als Kommunikationsvermittler. Damit die Koordination bei den verschiedenen Vorgängen, wie sie in einer Vielzahl von Abteilungen und

Organisationen vorkommen, reibungslos funktioniert, müssen daher den einzelnen Teammitgliedern bestimmte Rollen und Verantwortungsbereiche zugewiesen werden. Nachstehend einige Beispiele hierfür.

Gruppe	Rollen und Verantwortungsbereiche
Zugehörige Interessengruppe	✓ Genehmigt den Kommunikationsplan ✓ Sorgt für geeignete Verbreitung der Kommunikation ✓ Sorgt für angemessene Unterstützung auf allen Ebenen ✓ Macht die Organisation für die Verbreitung von Informationen verantwortlich
Träger der Sensibilisierungsmaßnahme	✓ Unterstützt die Kommunikationsstrategie und sorgt für angemessene Unterstützung der Projekte ✓ Unterstützt das Sensibilisierungsforum aktiv im Hinblick auf die Abstimmung mit den Zielen der Führungsebene ✓ Stellt angemessene Ressourcen zur Verfügung
Sensibilisierungsteam	✓ Übernimmt Führungsverantwortung und entwickelt Kommunikationsstrategie und -plan ✓ Führt die von Fachleuten im Rahmen des Programms erarbeiteten Inhalte zusammen ✓ Entwickelt Kommunikationsinhalte gemäß dem Kommunikationsplan und setzt diese gegebenenfalls um ✓ Sorgt für plangemäße Durchführung aller erforderlichen Kommunikationsmaßnahmen

Beispiel

Kommunikationsplan im Detail festlegen

Sobald Ziele, Kanäle, zentrale Botschaften, Rollen und Verantwortungsbereiche für die Kommunikation eindeutig festgelegt sind, kann das Sensibilisierungsteam einen detaillierten Kommunikationsplan erstellen. Bei der Ausarbeitung und Umsetzung einer zielgerichteten Kommunikationsstrategie und entsprechender Pläne geht es darum, den Grad der Sensibilisierung in den ermittelten Zielgruppen zu bestimmen, die Zielgruppen anzusprechen und eine erhöhte Sensibilisierung herbeizuführen.

Der Kommunikationsplan dient als Hilfsmittel, um die Zielgruppen strukturiert anzusprechen, und er verringert die Wahrscheinlichkeit, dass wichtige Interessengruppen außer Acht gelassen werden. Kommunikationspläne sind in der Regel auf ein Jahr angelegt (mit Aktualisierung nach Bedarf); in ihnen werden alle Maßnahmen für sämtliche Zielgruppen koordiniert. Dadurch wird auch vermieden, dass durch Koordinationslücken Doppelaufwand entsteht. Nachstehend ein Auszug aus einem Kommunikationsplan als Beispiel.

Ziel-gruppe	Bedürfnisse der Zielgruppe	Botschaft	Kanal	Verant-wortung	Ziele	Zeitplan/ Frequenz	Feedback-instrument
An wen richtet sich die Botschaft?	Kommuni-kations-bedürfnisse der Zielgruppe	Kommuni-kationsinhalt	Vermittlung der Botschaft	Wer ist für die Kommu-nikation verant-wortlich?	Was soll durch die Kommuni-kation erreicht werden?	Wann soll die Kommuni-kation stattfinden?	Wie wird Feedback eingeholt?
Silver Surfer	Geringe bis gar keine Vorkenntnisse Sind ohne IKT	Schutz personen-bezogener Daten im Internet	Informations verbreitung über Gesund-heitsein-	Sensibili-sierungs-team	Verständnis für die Problematik und Kenntnis	In zeitlicher Abstimmung mit der landesweiten Woche der	E-Mail Telefon

	aufgewachsen, daher eventuell Misstrauen gegenüber der Technik		richtungen Information in Zusammen-arbeit mit der Sozial-versicherung		möglicher Lösungen	älteren Mitbürger	

Erfolgsindikatoren für das Programm festlegen

Anhand geeigneter Indikatoren kann gemessen werden, wie effizient ein Sensibilisierungsprogramm ist und inwieweit es geeignet ist, die Informationssicherheit zu verbessern.([29]) Dass Sicherheitsbewusstsein wichtig ist, steht außer Zweifel, doch haben bisher nur wenige öffentliche oder private Organisationen den Versuch unternommen, den Wert bzw. die Effektivität eines Sensibilisierungsprogramms zu quantifizieren.

Die Evaluierung einer Kampagne oder eines Programms ist Voraussetzung für eine Bewertung der Effektivität der Initiative; außerdem können die dabei gewonnenen Daten als Leitparameter für die weitere Optimierung genutzt werden. Hierbei ist allerdings zu beachten, dass die für die Evaluierung verwendeten Messgrößen nicht für alle Zielgruppen gleichermaßen angewandt werden können, da sich Bedürfnisse und Ausgangssituation der einzelnen Zielgruppen zum Teil erheblich unterscheiden.

Welche Indikatoren gibt es?

Als Indikatoren werden Messgrößen und Schlüsselleistungsindikatoren verwendet; diese lassen sich wie folgt definieren:

Flughafenbetreiber – Die Rolle von Messgrößen und Audits

Flughafenbetreiber sehen sich einer wachsenden Bedrohung durch Terrorismus und andere Gefahren ausgesetzt. Die Unternehmen übermitteln regelmäßig große Mengen an Informationen zwischen ihren eigenen Systemen und Systemen Dritter. Die wichtigsten Kontrollsysteme sind untereinander vernetzt. Aus all diesen Aspekten zusammen ergibt sich, dass Informationssicherheit für Flughafenbetreiber ein wesentlicher Faktor ist

Die Beschäftigten am Flughafen haben unterschiedlichste soziale Hintergründe, vielfach handelt es sich um Zeitarbeitskräfte oder Mitarbeiter von Zulieferfirmen. Die Betreiberunternehmen setzen daher auf eine Vielzahl verschiedener Verfahren, um das Sicherheitsbewusstsein zu schärfen. Da nicht alle Mitarbeiter über gute IT-Kenntnisse verfügen, haben sich regelmäßige E-Mails und andere Mitteilungen zum Thema als sehr wirksam erwiesen. Durch die Beobachtung von Vorfällen innerhalb und außerhalb der Organisation können die Leitlinien stets auf dem aktuellen Stand gehalten werden.

Vorschriften und Verfahrensanweisungen entsprechen den maßgeblichen ISO-Normen. Dadurch allein konnte das Bewusstsein jedoch nicht verbessert werden. Vorschriften sind zwar ein notwendiger Bestandteil des Kontrollrahmens, erfreuen sich bei den Mitarbeitern aber nur geringer Beliebtheit.

Soweit dies machbar war, wurden Anforderungen aus den Vorschriften in elektronische oder automatisierte Prozesse integriert. Dies hilft den Mitarbeitern dabei, die Vorschriften einzuhalten, und es können genauere Tätigkeitsprotokolle erstellt werden als bei entsprechenden manuellen Prozessen. Anhand der Protokolle lässt sich einfach überprüfen, ob die Mitarbeiter die Vorschriften einhalten.

Internen und externen Audits kommt bei der Überprüfung von Verhaltensweisen und der Einhaltung von Prozessen und Vorschriften eine wichtige Rolle zu. Durch die Audits lässt sich feststellen, in welchen Bereichen es noch an Bewusstsein für bewährte Verfahrensweisen oder Vorschriften fehlt. Da die Auditberichte der Unternehmensleitung vorgelegt werden, werden Mängel ernst genommen. Dadurch werden Genehmigungen für neue Sicherheitsinitiativen und Sensibilisierungsmaßnahmen schneller erteilt.

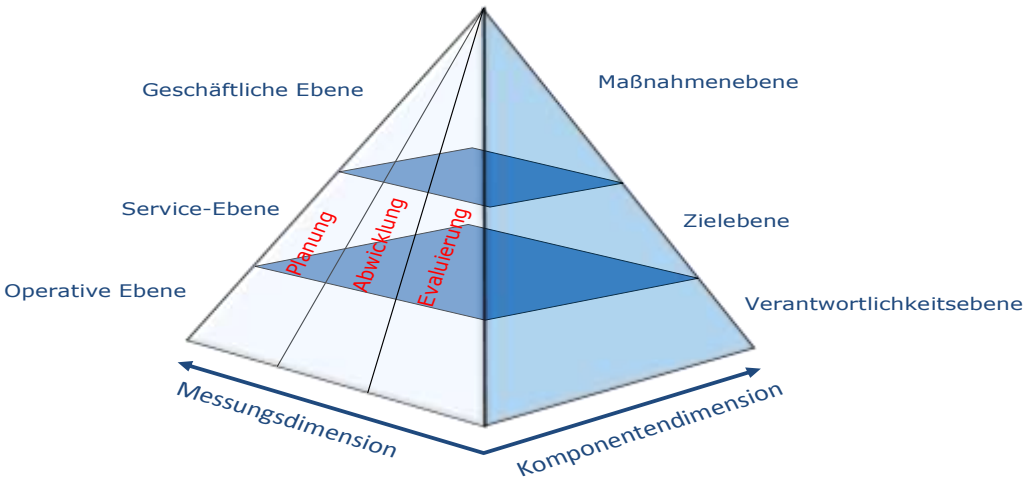
Die Verfolgung von Vorfällen gibt auch Aufschluss über den Grad des Sicherheitsbewusstseins. Durch die Überprüfung der Ursachen von Vorfällen und Ausfallzeiten können Verhaltenstendenzen ermittelt werden. Diese werden analysiert, um Defizite bei der Sensibilisierung oder Fortbildung aufzudecken und bei der Planung künftiger Initiativen zu berücksichtigen.

([29]) ENISA, *Sensibilisierungsmaßnahmen zur Informationssicherheit: Die übliche Praxis und die Erfolgsmessung*, 2007, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/kpi/measuring_aw_de.pdf

- ✓ Messgrößen: ein System von Parametern oder Methoden zur quantitativen Bewertung eines zu messenden Prozesses sowie die Prozesse, mit denen diese Messung durchgeführt wird. Messgrößen können aufgrund gewonnener Erkenntnisse im Laufe der Zeit weiterentwickelt und verändert werden. Es gibt unabhängige Messgrößen und Messgrößen, die sich wechselseitig beeinflussen. Die Messgrößen können durch Schlüsselleistungsindikatoren weiter untergliedert oder detailliert werden.
- ✓ Schlüsselleistungsindikatoren (key performance indicators, KPI): quantifizierbare Messgrößen, die dazu verwendet werden, die Leistung einer Organisation anhand der Zielvorgaben zu bewerten. Die KPI richten sich nach der jeweiligen Organisation; hierbei sind verschiedene Ebenen und Dimensionen zu berücksichtigen. KPI können sowohl für quantitative als auch für qualitative Messungen herangezogen werden, aussagekräftig sind sie jedoch vor allem für quantitative Messungen, für die sie auch zumeist verwendet werden. Entsprechende Messungen betreffen unter anderem die Zahl der als Zielgruppe angesprochenen Bürger, die Zahl der Sicherheitsvorfälle im zurückliegenden Jahr im Vergleich zum Vorjahr sowie die Zahl der Aufrufe einer Website.

Für die Festlegung von Leistungszielen und Leistungsmessungen (u. a. unter Verwendung von Messgrößen und KPI) können verschiedene industrieübliche Leistungsmanagementmodelle, wie z. B. „Balanced Scorecard" oder „Six Sigma", verwendet werden.

Bei der Festlegung von Messgrößen und KPI sind verschiedene Ebenen und Dimensionen zu beachten – siehe Beispiel unten.



Ebene	Beschreibung	Beispiel
Geschäftliche Ebene	Messung der Auswirkungen der Funktion als Ganzes (z. B. Finanzwesen, Personalwesen) auf die Geschäftsziele	✓ Kundenzufriedenheit ✓ Mitarbeiterzufriedenheit ✓ Geschäftsspezifische Ergebnisse ✓ Finanzielle Verhältniszahlen (z. B. Kosten je VZÄ)

Service-Ebene	Messung der Tätigkeiten und Arbeitsergebnisse, die die Dienstleistung ausmachen	✓ Service Level Agreement (SLA) / Dienstgütevereinbarung (DGV) ✓ Operator Level Agreement (OLA) (Zusatzvertrag zu SLA/DGV)
Operative Ebene	Detaillierte Prozesse oder technische Messungen, die für die betrieblichen Abläufe der Organisation erforderlich sind	✓ Fehlerquote bei Batch-Prozess x ✓ Zeitaufwand für die Einhaltung des Verfahrens

Dimension	Beschreibung
Planung	Planung aller Aktivitäten, die mit einer Initiative bzw. einem Programm zur verstärkten Sensibilisierung für Informationssicherheit im Zusammenhang stehen.
Abwicklung	Ausführung und Abwicklung aller Aktivitäten, die mit einer Initiative bzw. einem Programm zur verstärkten Sensibilisierung für Informationssicherheit im Zusammenhang stehen.
Evaluierung	Bewertung und gegebenenfalls Anpassung aller Aktivitäten, die mit einer Initiative bzw. einem Programm zur verstärkten Sensibilisierung für Informationssicherheit im Zusammenhang stehen.

Nachstehend einige Indikatoren:

Nr.	Schlüsselleistungsindikatoren (*)
1	Budgetanteil, der für Schulungsmaßnahmen zur Sensibilisierung ausgegeben wird (in %)
2	Arbeitszeitanteil je VZÄ, der für Schulungsmaßnahmen zur Sensibilisierung aufgewendet wird (in %)
3	Alter der Beschäftigten, die an Schulungsmaßnahmen zur Sensibilisierung teilnehmen/Durchschnittsalter aller Beschäftigten
4	Zykluszeit in Tagen von der Organisation von Sensibilisierungsmaßnahmen bis zum Abschluss der Kampagne
5	Anzahl VZÄ mit Sicherheitsschulung/Nutzer insgesamt
6	Anzahl qualifizierter Aufrufe/Monat
7	Gesamtkosten der Sensibilisierungsinitiative pro Jahr
8	Gesamtkosten der Schulungsmaßnahmen zur Sensibilisierung je VZÄ
9	Personalkosten insgesamt für Planung und Abwicklung von Sensibilisierungsinitiativen
10	Kundenzufriedenheit mit Leistungserbringung (d. h. Pünktlichkeit und Qualität) (in %)
11	Fähigkeit der Mitarbeiter, Rollen auszufüllen (in %)
12	Mitarbeiterzufriedenheit (in %)
13	Zugewinn an Selbstvertrauen der älteren Mitarbeiter (in %)
14	Anteil der leitenden Führungskräfte/Führungskräfte, Angehörigen der mittleren Führungsebene/Fachkräfte, Sachbearbeiter, die an Managemententwicklungsprogrammen teilgenommen haben (in %)
15	Anteil der leitenden Führungskräfte/Führungskräfte, Angehörigen der mittleren Führungsebene/Fachkräfte, Sachbearbeiter, die eine Sicherheitsüberprüfung absolviert haben (in %)

16	Anteil der erreichten Zielvorgaben für die Leistungserbringung (in %)
17	Zufriedenheit der Interessengruppen mit der Kommunikation über das Programm (in %)
18	Zufriedenheit der Interessengruppen mit den Governance-Regelungen (in %)
19	Anteil der Interessengruppen, die den Nutzen der Initiative verstehen/erkennen (in %)
20	Widerstand der Interessengruppen gegen Veränderungen (in %)
21	Zufriedenheit der Interessengruppen damit, inwieweit das System in der Lage ist, die geschäftlichen Anforderungen zu erfüllen (in %)
22	Anteil der Mitarbeiter, die ihre Rolle bei der Verwirklichung der Sicherheitsziele verstehen (in %)
23	Durchschnittliche Anzahl Schulungstage je Mitarbeiter
24	Durchschnittliche Personalkosten je VZÄ für den Prozess „Veränderungsmanagement"
25	Durchschnittliche Personalkosten je VZÄ für den Prozess „Verstärkte Sensibilisierung"
26	Häufigkeit/Relevanz von Befragungen
27	Anzahl der Vorteile/Nutzen gemäß Geschäftsszenario
28	Anzahl Mitarbeiter je VZÄ „Lernen durch Entwicklung und Beratung"
29	Anzahl der Veränderungen bei den Rollen der Führungskräfte
30	Anzahl der Veränderungen bei Tätigkeiten der Mitarbeiter
31	Anzahl der richtigen Antworten bei Sicherheitsselbstbewertungen/Fragen insgesamt
32	Anzahl der für die Entwicklung zuständigen Mitarbeiter/Mitarbeiter insgesamt
33	Anzahl VZÄ für den Prozess „Lernen durch Entwicklung und Beratung" je 1 000 EUR laufender Betriebskosten
34	Anzahl Teilnehmer an der Umfrage zur Sensibilisierung/Mitarbeiter insgesamt
35	Anzahl der durchgeführten Sicherheitsselbstbewertungen/Jahr
36	Gesamtkosten für den Prozess „Lernen durch Entwicklung und Beratung" je 1 000 EUR laufender Betriebskosten
37	Interne Personalkosten insgesamt für den Prozess „Lernen durch Entwicklung und Beratung" je 1 000 EUR laufender Betriebskosten
38	Beitrag der IKT-Schulung zur Wertschöpfung je Mitwirkenden in Prozentpunkten
39	Anzahl der Mitarbeiter, die die Prüfung bestanden bzw. Zertifizierung erhalten haben/Mitarbeiter insgesamt
40	Anzahl der Organisationen, die das Instrumentarium übernehmen/Jahr
41	Anzahl der Personen, die die Prüfung bestanden bzw. Zertifizierung erhalten haben/befragte Personen insgesamt
42	Anzahl Downloads des Instrumentariums/Monat
43	Anzahl der Themen im Bereich Sicherheit an weiterführenden Schulen und Hochschulen/Themen insgesamt
44	Anzahl der Themen im Bereich Sicherheit im Primar- und Sekundarschulwesen/Themen insgesamt
45	Budgetanteil, der für Schulungsmaßnahmen zur Sensibilisierung ausgegeben wird (in %)
46	Anteil der Mitarbeiter, die nach 1950 geboren sind (in %)
47	Anteil der Unternehmen mit 10 oder mehr Beschäftigten, die das Internet nutzen (in %)
48	Anzahl der Internetzugänge insgesamt/je 100 Einwohner
49	Anzahl der Haushalte mit PC-Zugang/Land
50	Anzahl der Haushalte mit Internetzugang/Land
51	Anzahl der Mobilfunkteilnehmer insgesamt/je 100 Einwohner
52	Anzahl der Breitbandnutzer insgesamt/je 100 Einwohner
53	Schulungskosten je VZÄ

54	Zykluszeit in Tagen für die Behebung eines Sicherheitsproblems
55	Durchschnittliche Zeit von der Feststellung bis zur Meldung einer neuen Bedrohung
56	Anzahl der ermittelten Störungen/Jahr
57	Anzahl der Alarmmeldungen, Warnungen, Meldungen, Empfehlungen/Monat
58	Anzahl der Kommunikationsvorgänge mit anderen Ländern/Jahr
59	Anzahl der Systeme ohne Passwortvorschriften/Systeme insgesamt
60	Anzahl der ausgestellten Token, Zertifikate, elektronischen Ausweise/Gesamtbevölkerung
61	Anzahl der gemeldeten Vorfälle je Kategorie/Jahr
62	Anzahl der von lokalen oder internationalen Unternehmen eingeführten Zertifizierungsprogramme
63	Anzahl der E-Government-Projekte, die nach den Standards durchgeführt werden/Projekte insgesamt
64	Anzahl der Ausgaben/Jahr
65	Anzahl der erfassten Veranstaltungen/Monat
66	Anzahl der verteilten Materialien/Ausgabe
67	Anzahl der verteilten Materialien/Jahr
68	Anzahl der Teilnehmer an Schulungsmaßnahmen zur Sensibilisierung je Kampagne
69	Anzahl der Schulungstage je Mitarbeiter/Jahr
70	Anzahl der einmaligen Besucher/Monat
71	Zeitaufwand für die Organisation einer Sensibilisierungsinitiative

(*) *Die meisten Schlüsselleistungsindikatoren werden nicht als absolute Zahlen, sondern als anteilige Verhältniszahlen ausgedrückt (z. B. Anzahl Einheiten je VZÄ oder je 1 000 EUR Ausgaben).*
VZÄ = Vollzeitäquivalent

Unterschiede bei den Zielgruppen berücksichtigen

Es muss bedacht werden, dass bei der Evaluierung nicht für alle Zielgruppen dieselben Messgrößen angewandt werden können, da sich die Zielgruppen hinsichtlich ihrer Interessen und Bedürfnisse, aber auch hinsichtlich der Nutzersituation zum Teil erheblich unterscheiden.

Bei der Festlegung von Messgrößen für die Evaluierung von Kampagnen, beispielsweise für die Zielgruppe der privaten PC-Nutzer oder der KMU (die beiden bei Initiativen zur Sensibilisierung für Informationssicherheit am häufigsten angesprochenen Zielgruppen), sind einige wichtige Punkte zu beachten:

- ✓ Der Schwerpunkt von Sensibilisierungsprogrammen für die Zielgruppe der KMU sollte darauf liegen, dass eine Informationssicherheitspolitik entwickelt und umgesetzt wird, sowie darauf, das für die Einhaltung dieser Politik im Unternehmen erforderliche Instrumentarium vorzuschlagen. Diese Empfehlung gilt auch für Organisationen im öffentlichen Sektor.
- ✓ Die Entwicklung einer Informationssicherheitspolitik für private PC-Nutzer fällt nicht in den Zuständigkeitsbereich einer Behörde. Deshalb sollte der Schwerpunkt vielmehr auf der Entwicklung von „empfohlenen Leitlinien" oder „beispielhaften Verhaltensweisen" zur Informationssicherheit und deren Verbreitung in der Öffentlichkeit liegen.

Zur genaueren Bestimmung der verschiedenen äußeren Einflüsse, denen die Zielgruppen ausgesetzt sind, können Hilfsmittel verwendet werden, die ansonsten hauptsächlich im Unternehmensbereich eingesetzt werden, wie z. B. die PESTEL-Analyse (PESTEL, Akronym für die englischen Begriffe *political, environmental, social, technological, economical and legal,* zu deutsch: politisch, ökologisch, soziokulturell, technologisch, ökonomisch und rechtlich).

Behörden sind nicht dafür zuständig, eine wie auch immer geartete Informationssicherheitspolitik für private PC-Nutzer zu entwickeln. Sie sollten sich deshalb darauf konzentrieren, „empfohlene Leitlinien" oder „beispielhafte Verhaltensweisen" zur Informationssicherheit zu erarbeiten und diese in der Öffentlichkeit zu propagieren.

Schlüsselleistungsindikatoren zu Prozessen und Ebenen zuordnen

Wenn zusätzlich zu den Prozessen und Aktivitäten Schlüsselleistungsindikatoren und Messgrößen festgelegt wurden, können die Indikatoren den jeweiligen Prozessen und Ebenen zugeordnet werden, die die Organisationen für die Erfüllung ihrer Aufgaben nutzen.

Durch diese Zuordnung wird sichergestellt, dass jeder wichtige Einzelschritt nachvollzogen und sein Erfolg gemessen wird. In der nachstehenden Tabelle ist das Ergebnis im Überblick dargestellt. Bei den KPI handelt es sich um die Indikatoren aus der Tabelle weiter oben in diesem Kapitel.

Ebene	Prozess	Nr.	Schlüsselleistungsindikatoren
Geschäftlich	Evaluierung	1	Budgetanteil, der für Schulungsmaßnahmen zur Sensibilisierung ausgegeben wird (in %)
Geschäftlich	Evaluierung	2	Arbeitszeitanteil je VZÄ, der für Schulungsmaßnahmen zur Sensibilisierung aufgewendet wird (in %)
Geschäftlich	Evaluierung	3	Alter der Beschäftigten, die an Schulungsmaßnahmen zur Sensibilisierung teilnehmen/Durchschnittsalter aller Beschäftigten
Geschäftlich	Evaluierung	4	Zykluszeit in Tagen von der Organisation von Sensibilisierungsmaßnahmen bis zum Abschluss der Kampagne
Geschäftlich	Evaluierung	5	Anzahl VZÄ mit Sicherheitsschulung/Nutzer insgesamt
Geschäftlich	Evaluierung	6	Anzahl qualifizierter Aufrufe/Monat
Geschäftlich	Evaluierung	7	Gesamtkosten der Sensibilisierungsinitiative pro Jahr
Geschäftlich	Evaluierung	8	Gesamtkosten der Schulungsmaßnahmen zur Sensibilisierung je VZÄ
Geschäftlich	Evaluierung	9	Personalkosten insgesamt für Planung und Abwicklung von Sensibilisierungsinitiativen
Geschäftlich	Evaluierung	10	Kundenzufriedenheit mit Leistungserbringung (d. h. Pünktlichkeit und Qualität) (in %)
Geschäftlich	Evaluierung	11	Fähigkeit der Mitarbeiter, Rollen auszufüllen (in %)
Geschäftlich	Evaluierung	12	Mitarbeiterzufriedenheit (in %)
Geschäftlich	Evaluierung	13	Zugewinn an Selbstvertrauen der älteren Mitarbeiter (in %)
Geschäftlich	Evaluierung	14	Anteil der Führungskräfte, Angehörigen der mittleren Führungsebene/Fachkräfte, Sachbearbeiter, die an Managemententwicklungsprogrammen teilgenommen haben (in %)
Geschäftlich	Evaluierung	15	Anteil der Führungskräfte, Angehörigen der mittleren Führungsebene/Fachkräfte, Sachbearbeiter, die eine Sicherheitsüberprüfung absolviert haben (in %)
Geschäftlich	Evaluierung	16	Anteil der erreichten Zielvorgaben für die Leistungserbringung (in %)
Geschäftlich	Evaluierung	17	Zufriedenheit der Interessengruppen mit der Kommunikation über das Programm (in %)

Geschäftlich	Evaluierung	18	Zufriedenheit der Interessengruppen mit den Governance-Regelungen (in %)
Geschäftlich	Evaluierung	19	Anteil der Interessengruppen, die den Nutzen der Initiative verstehen/erkennen (in %)
Geschäftlich	Evaluierung	20	Widerstand der Interessengruppen gegen Veränderungen (in %)
Geschäftlich	Evaluierung	21	Zufriedenheit der Interessengruppen damit, inwieweit das System in der Lage ist, die geschäftlichen Anforderungen zu erfüllen (in %)
Geschäftlich	Evaluierung	22	Anteil der Mitarbeiter, die ihre Rolle bei der Verwirklichung der Sicherheitsziele verstehen (in %)
Geschäftlich	Evaluierung	23	Durchschnittliche Anzahl Schulungstage je Mitarbeiter
Geschäftlich	Evaluierung	24	Durchschnittliche Personalkosten je VZÄ für den Prozess „Veränderungsmanagement“
Geschäftlich	Evaluierung	25	Durchschnittliche Personalkosten je VZÄ für den Prozess „Verstärkte Sensibilisierung“
Geschäftlich	Evaluierung	26	Häufigkeit/Relevanz von Befragungen
Geschäftlich	Evaluierung	27	Anzahl der Vorteile/Nutzen gemäß Geschäftsszenario
Geschäftlich	Evaluierung	28	Anzahl Mitarbeiter je VZÄ „Lernen durch Entwicklung und Beratung“
Geschäftlich	Evaluierung	29	Anzahl der Veränderungen bei den Rollen der Führungskräfte
Geschäftlich	Evaluierung	30	Anzahl der Veränderungen bei Tätigkeiten der Mitarbeiter
Geschäftlich	Evaluierung	31	Anzahl der richtigen Antworten bei Sicherheitsselbstbewertungen/Fragen insgesamt
Geschäftlich	Evaluierung	32	Anzahl der für die Entwicklung zuständigen Mitarbeiter/Mitarbeiter insgesamt
Geschäftlich	Evaluierung	33	Anzahl VZÄ für den Prozess „Lernen durch Entwicklung und Beratung“ je 1 000 EUR laufender Betriebskosten
Geschäftlich	Evaluierung	34	Anzahl Teilnehmer an der Umfrage zur Sensibilisierung/Mitarbeiter insgesamt
Geschäftlich	Evaluierung	35	Anzahl der durchgeführten Sicherheitsselbstbewertungen/Jahr
Geschäftlich	Evaluierung	36	Gesamtkosten für den Prozess „Lernen durch Entwicklung und Beratung“ je 1 000 EUR laufender Betriebskosten
Geschäftlich	Evaluierung	37	Interne Personalkosten insgesamt für den Prozess „Lernen durch Entwicklung und Beratung“ je 1 000 EUR laufender Betriebskosten
Service	Evaluierung	38	Beitrag der IKT-Schulung zur Wertschöpfung je Mitwirkenden in Prozentpunkten
Service	Evaluierung	39	Anzahl der Mitarbeiter, die die Prüfung bestanden bzw. Zertifizierung erhalten haben/Mitarbeiter insgesamt
Service	Evaluierung	40	Anzahl der Organisationen, die das Instrumentarium übernehmen/Jahr
Service	Evaluierung	41	Anzahl der Personen, die die Prüfung bestanden bzw. Zertifizierung erhalten haben/befragte Personen insgesamt
Service	Evaluierung	42	Anzahl Downloads des Instrumentariums/Monat
Service	Evaluierung	43	Anzahl der Themen im Bereich Sicherheit an weiterführenden Schulen und Hochschulen/Themen insgesamt

Service	Evaluierung	44	Anzahl der Themen im Bereich Sicherheit im Primar- und Sekundarschulwesen/Themen insgesamt
Geschäftlich	Planung	45	Budgetanteil, der für Schulungsmaßnahmen zur Sensibilisierung ausgegeben wird (in %)
Geschäftlich	Planung	46	Anteil der Mitarbeiter, die nach 1950 geboren sind (in %)
Operativ	Planung	47	Anteil der Unternehmen mit 10 oder mehr Beschäftigten, die das Internet nutzen (in %)
Operativ	Planung	48	Anzahl der Internetzugänge insgesamt/je 100 Einwohner
Operativ	Planung	49	Anzahl der Haushalte mit PC-Zugang/Land
Operativ	Planung	50	Anzahl der Haushalte mit Internetzugang/Land
Operativ	Planung	51	Anzahl der Mobilfunkteilnehmer insgesamt/je 100 Einwohner
Operativ	Planung	52	Anzahl der Breitbandnutzer insgesamt/je 100 Einwohner
Geschäftlich	Planung/Evaluierung	53	Schulungskosten je VZÄ
Operativ	Planung/Evaluierung	54	Zykluszeit in Tagen für die Behebung eines Sicherheitsproblems
Operativ	Planung/Evaluierung	55	Durchschnittliche Zeit von der Feststellung bis zur Meldung einer neuen Bedrohung
Operativ	Planung/Evaluierung	56	Anzahl der ermittelten Störungen/Jahr
Operativ	Planung/Evaluierung	57	Anzahl der Alarmmeldungen, Warnungen, Meldungen, Empfehlungen/Monat
Operativ	Planung/Evaluierung	58	Anzahl der Kommunikationsvorgänge mit anderen Ländern/Jahr
Operativ	Planung/Evaluierung	59	Anzahl der Systeme ohne Passwortvorschriften/Systeme insgesamt
Operativ	Planung/Evaluierung	60	Anzahl der ausgestellten Token, Zertifikate, elektronischen Ausweise/Gesamtbevölkerung
Operativ	Planung/Evaluierung	61	Anzahl der gemeldeten Vorfälle je Kategorie/Jahr
Service	Planung/Evaluierung	62	Anzahl der von lokalen oder internationalen Unternehmen eingeführten Zertifizierungsprogramme
Service	Planung/Evaluierung	63	Anzahl der E-Government-Projekte, die nach den Standards durchgeführt werden/Projekte insgesamt
Geschäftlich	Planung/Abwicklung/Evaluierung	64	Anzahl der Ausgaben/Jahr
Geschäftlich	Planung/Abwicklung/Evaluierung	65	Anzahl der erfassten Veranstaltungen/Monat
Geschäftlich	Planung/Abwicklung/Evaluierung	66	Anzahl der verteilten Materialien/Ausgabe
Geschäftlich	Planung/Abwicklung/Evaluierung	67	Anzahl der verteilten Materialien/Jahr
Geschäftlich	Planung/Abwicklung/Evaluierung	68	Anzahl der Teilnehmer an Schulungsmaßnahmen zur Sensibilisierung je Kampagne
Geschäftlich	Planung/Abwicklung/Evaluierung	69	Anzahl der Schulungstage je Mitarbeiter/Jahr
Geschäftlich	Planung/Abwicklung/Evaluierung	70	Anzahl der einmaligen Besucher/Monat
Geschäftlich	Planung/Abwicklung/Evaluierung	71	Zeitaufwand für die Organisation einer Sensibilisierungsinitiative

VZÄ = Vollzeitäquivalent

Ausgangsbasis der Evaluierung bestimmen

Im vorhergehenden Kapitel ging es um Messgrößen für die Evaluierung der Effektivität eines Sensibilisierungsprogramms. Als Ausgangsbasis für die Verwendung dieser Messgrößen muss

allerdings zunächst eine Bestandsaufnahme der Ist-Situation vorgenommen werden. Die Bestimmung der Ausgangsbasis hilft dabei, die bestehenden Aktivitäten zur Informationssicherheit innerhalb der Organisation einer Prüfung zu unterziehen, mögliche Defizite in einzelnen Bereichen oder bei bestimmten Themen zu ermitteln, die Unterstützung der Führungsebene und damit letztlich auch Finanzmittel zu bekommen, Aktivitäten und Aufklärungsmaßnahmen nach ihrer Priorität zu ordnen und die Fortschritte gegenüber der Ausgangssituation zu verfolgen.

Durch diese Bestandsaufnahme im Vorfeld wird es zudem möglich, den Nutzen, den das Sensibilisierungsprogramm bewirkt, zu bestimmen und zu verfolgen. Eine Evaluierung bietet eine ideale Gelegenheit zu beurteilen, bei welchen Komponenten des Programms die Erfolgsrate besonders hoch bzw. besonders gering ausgefallen ist.

Anhand von Fragebogen und Mehrthemenbefragungen lässt sich die Effektivität von Sensibilisierungsprogrammen evaluieren. Da bei künftigen Evaluierungen diese Ausgangsbasis zugrunde gelegt wird, muss darauf geachtet werden, in späteren Stadien der Initiative möglichst ähnliche Fragebogen und Befragungen zu verwenden.

Eine Bestandsaufnahme, in die alle Aspekte einfließen, die mit der Sensibilisierung für Informationssicherheit in Zusammenhang stehen, trägt dazu bei, Defizite in einzelnen Bereichen und bei bestimmten Themen aufzudecken sowie aktuelle Sachstandsberichte zu Initiativen und Aktivitäten der Organisation auf dem Gebiet zu erstellen. Fragebogen und Mehrthemenbefragungen bieten zudem die Möglichkeit, die Effektivität der Programme zu evaluieren.

Arbeitsblätter zur Bestandsaufnahme und zur Bestimmung der Ausgangsbasis sowie ein Musterfragebogen zur Sensibilisierung sind in den Anhängen VI, VII und VIII zu finden.

Gewonnene Erfahrungen dokumentieren

Nach Durchführung aller Einzelschritte dieser ersten Phase sollte Zeit eingeplant werden, um zu ermitteln, welche Erfahrungen bis hierher gewonnen wurden, und diese Erfahrungen zu dokumentieren. Der nachstehend beschriebene Prozess dient als Beispiel dafür, wie gewonnene Erfahrungen ermittelt, dokumentiert und weitergegeben werden können. Dies besagt jedoch nicht, dass Erfahrungen nur als Ergebnis eines Gruppenprozesses dokumentiert werden können.

Je nach Umfeld und äußeren Gegebenheiten, in denen das Programm durchgeführt wird, sollte es ein Instrument geben, mit dem die einzelnen Mitglieder des Programmteams Aktennotizen oder längere Vermerke festhalten und an eine bestimmte Person weiterleiten können, die diese Unterlagen dann aufbereitet und in einem Speicher oder einer Datenbank ablegt. Ein entsprechender Prozess sollte als Ergebnis von Schritt 1 des Verfahrens festgelegt und dokumentiert werden.

Wichtige Überlegungen

Wenn zu Beginn der Besprechung die Grundregeln festgelegt werden, muss unter anderem angesprochen werden, was unter einer „Besprechung über die gewonnenen Erfahrungen" bzw. Nachbesprechung verstanden wird und wie konstruktive Kritik geübt wird. Hier einige Grundsätze für konstruktives Feedback:

- ✓ Die gewonnenen Erfahrungen sollen den Blick auf die Abwicklung des Programms und nicht auf die Arbeitsergebnisse lenken.
- ✓ Fallbeispiele eignen sich besonders gut, um Argumente anschaulich zu machen.
- ✓ Kritik muss konstruktiv sein und sollte sich auf einen Prozess, nicht jedoch auf Personen beziehen. Die Teilnehmer werden angehalten, bei ihrem Feedback hierauf zu achten.
- ✓ Wenn keine Aussicht besteht, einen Kritikpunkt zu klären, Abhilfe zu schaffen oder anderweitig zu beeinflussen, sollte nicht darüber diskutiert werden.
- ✓ Durch individuelle Sitzungsvorbereitung lässt sich der Prozess beschleunigen.
- ✓ Denken Sie daran, dass dieses Forum sowohl der Kritik als auch dem Lob dient – nehmen Sie beides nicht allzu persönlich, denn es geht um das Team.
- ✓

Eine Nachbesprechung bietet möglicherweise Gelegenheit, verschiedene organisatorische Ziele zu erreichen:

- ✓ Über alternative Konzepte zu den derzeitigen Prozessen und zur Verbesserung des Programms in seiner derzeitigen Form zu diskutieren.
- ✓ Den Mitarbeitern zu zeigen, dass ihre Beiträge geschätzt und beachtet werden.
- ✓ Die Moral des Teams zu stärken.
- ✓ Die bei diesem Programm gewonnenen Erfahrungen können in zukünftige Programme mit ähnlicher Zielsetzung einfließen.

Eine hervorragende Gelegenheit für Feedback und Verbesserungen

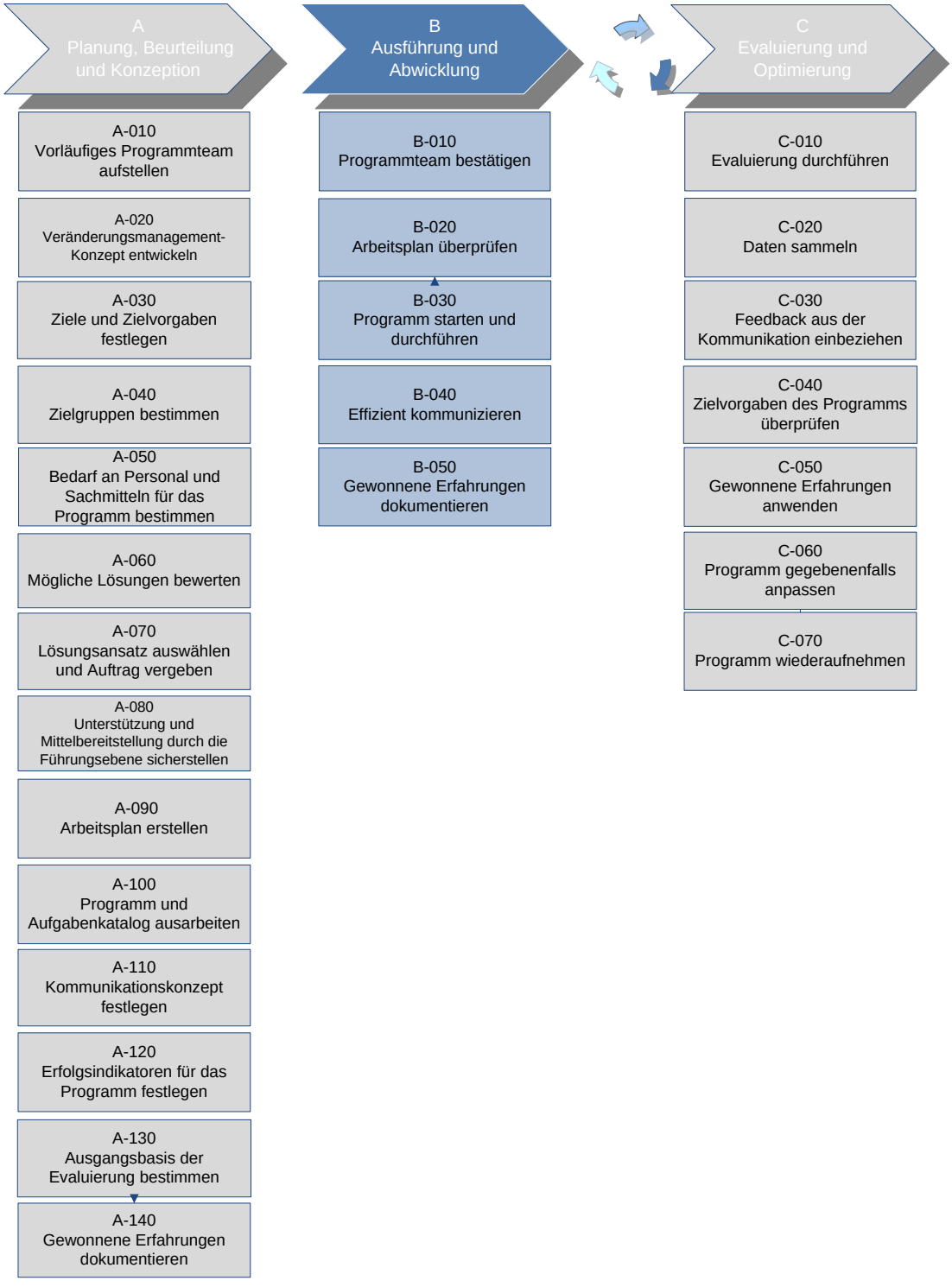
Zuweilen haben Mitarbeiter sehr genaue Vorstellungen davon, wie bestimmte Teile eines Programms abgewickelt werden sollten. Dieses Forum bietet eine hervorragende Gelegenheit, Meinungen weiterzugeben, andere Ideen aufzugreifen und unterschiedliche Ansätze für die laufenden Prozesse zu diskutieren. Ein geschickter Moderator versteht es, die Besprechung so zu lenken, dass die Teammitglieder Frustrationen abbauen und positiv und konstruktiv umsetzen können und dass ein Feedback zustande kommt, das im weiteren Verlauf zur Verbesserung der Prozesse beiträgt.
Der Programmmanager oder Teamleiter muss in der Lage sein, die in die Besprechung hineingetragenen Erwartungen wirksam zu lenken und die bei der Nachbesprechung hervorgehobenen positiven Aspekte mit den Vorgaben des Programmzeitplans in Einklang zu bringen. Gelingt dies nicht, besteht die Gefahr, dass die Nachbesprechung kontraproduktive Wirkung zeigt und die Moral des gesamten Teams beeinträchtigt. Innerhalb des Teams wird möglicherweise angenommen, dass die aufgezeigten Verbesserungen noch im laufenden Programm umgesetzt werden. Wenn jedoch die Zeit nicht ausreicht, die empfohlenen Veränderungen (gewonnenen Erfahrungen) im laufenden Programm aufzugreifen, sollte dies im Vorhinein mitgeteilt werden.
Es kann vorkommen, dass das Team einen Aspekt ermittelt hat, der eine Verbesserung des Ablaufs bewirken könnte, es jedoch zu diesem Zeitpunkt der Programmdurchführung zu zeit- und ressourcenaufwändig wäre, den neuen Prozess einzuführen (in diesem Fall würde durch die vermeintliche Verbesserung eher eine Verschlechterung bewirkt).
Für das Programmmanagement bergen die gewonnenen Erfahrungen sowohl positive als auch negative Aspekte. Bei der Dokumentation sollte daher sowohl festgehalten werden, was sich als gut erwiesen hat und in zukünftigen Programmen wiederholt werden sollte, als auch was nicht so gut gelaufen ist bzw. schieflaufen könnte und wie sich derartige Situationen zukünftig vermeiden bzw. ausschalten lassen.

Tipps für konstruktive Feedback-Besprechungen

- ✓ Setzen Sie ein Zeitlimit. Nachbesprechungen sind oft produktiv, aber zeitaufwändig. Wenn vorher ein Zeitlimit für die Beantwortung von Fragen festgelegt wird, wird auch in einer eher unstrukturierten oder freien Besprechung eine gewisse Ordnung gewahrt.
- ✓ Fordern Sie die Teammitglieder auf, ihre Gedanken bereits vor der Besprechung zu ordnen und zu Papier zu bringen. Wenn der Meinungsaustausch ins Stocken gerät, bringen Sie früher aufgetretene Schwierigkeiten und deren Behebung ins Gespräch. Verbesserungspotenzial findet sich häufig in Notizen aus Statusbesprechungen oder Problemprotokollen.
- ✓ Wenn gewonnene Erfahrungen nicht gleich schriftlich festgehalten werden, geraten sie beim Einzelnen meist in Vergessenheit.
- ✓ Die Teammitglieder sollten dazu ermuntert werden, während des Programms eine Art Logbuch oder Tagebuch zu führen, das sie dann zur Vorbereitung auf eine Nachbesprechung heranziehen können. Allerdings sollten die Teammitglieder dazu angehalten werden, Kommentare und Einträge ins Logbuch oder Tagebuch sachlich zu formulieren, da diese Unterlagen möglicherweise später in die Programmdokumentation aufgenommen werden.
- ✓ In den Statusbericht sollte eine Rubrik „Gewonnene Erfahrungen" aufgenommen werden, sodass die Erfahrungen am Ende einer Phase oder eines Programms leicht aufzufinden sind.
- ✓ Legen Sie den Zeitpunkt für die Aufarbeitung der gewonnenen Erfahrungen nach strategischen Gesichtspunkten fest. Besonders geeignete Zeitpunkte, zu denen Erfahrungen zur Verbesserung des Programmmanagements ermittelt werden können, sind das Ende eines Programms oder einer Programmphase, ein wichtiger Meilenstein, die Aufnahme oder Abgabe von Programmmitarbeitern und der Zeitpunkt nach einer Leistungsbewertung. Zu diesen Zeitpunkten sind die verbesserungswürdigen Prozesse den Beteiligten noch in lebhafter Erinnerung. Wie oft derartige Nachbesprechungen angesetzt werden, hängt von Umfang und Komplexität des Programms ab.
- ✓ Bei langfristig angelegten oder komplexen Programmen müssen gegebenenfalls regelmäßige Nachbesprechungen anberaumt werden, bei kleineren Programmen genügt unter Umständen eine einzige Nachbesprechung. Vor Beginn des Programms sollten Sie einen Lenkungsprozess für die Aufnahme von gewonnenen Erfahrungen festlegen, über den Sie das Team vorab informieren. Beispielsweise: Muss eine Besprechung anberaumt werden und müssen die gewonnenen Erfahrungen offiziell erfasst werden, bevor sie dem Programmmanagement vorgetragen werden, oder können die Teammitglieder ihre programmrelevanten Erfahrungen ad hoc vortragen? Die Vorgehenswiese richtet sich dabei im Wesentlichen nach der Erfahrung der Teammitglieder und dem Urteilsvermögen des Programmmanagers.
- ✓ Aufschlussreich ist möglicherweise auch der Austausch mit anderen Teams, die auch zu Nachbesprechungen eingeladen werden können, um über ähnlich gelagerte Erfahrungen zu sprechen, die gegebenenfalls aufgegriffen werden können.

Wichtig ist, gewonnene Erfahrungen zu ermitteln, zu dokumentieren und weiterzugeben. Für ein effektives Vorgehen empfiehlt sich die Verwendung einer geeigneten Software oder eines Formulars. Anhang IX enthält eine Vorlage für ein solches Formular zur Erfassung gewonnener Erfahrungen.

Phase II – Ausführung und Abwicklung



Programmteam bestätigen

In der zweiten Phase beginnt die Ausführung des Programms. Jedes Mitglied des Sensibilisierungsteams übernimmt bei der Umsetzung und Abwicklung der Initiative eine bestimmte Rolle. Vor dem eigentlichen Programmstart muss nun noch das Team bestätigt werden, das die Verantwortung für Ausführung und Ergebnisse des Programms trägt.

Arbeitsplan überprüfen

Vor Programmbeginn wird der Arbeitsplan nochmals auf den neuesten Stand gebracht und die Meilensteine des Programms so festgelegt, dass sie den Zielen und Zielvorgaben des Programms sowie den Budgetvorgaben entsprechen.

Der Arbeitsplan dient auch zur Verfolgung des Programmfortschritts. Hierbei könnte das Geschäftsszenario auch dazu genutzt werden, die Projektausführung und die Realisierung von Vorteilen zu lenken und zu beurteilen.

Programm starten und durchführen

Die vorgenannten Schritte und die Aktivitäten der vorhergehenden Phase wirken möglicherweise langwierig und bürokratisch, doch macht sich die Zeit, die für die Festlegung der Anforderungen, die Konzeption der Lösung und die Optimierung des erwarteten Ergebnisses aufgewendet wird, später mit Sicherheit bezahlt, wenn das Programm ohne große Reibungsverluste und effektiv durchgeführt werden kann.

Nachdem ein sorgsam konzipierter Plan ausgearbeitet wurde und die erforderlichen Ressourcen bereitstehen, ist es nunmehr an der Zeit, die Unterstützung der Kollegen intern und der ausgewählten Zulieferer extern einzufordern, damit das Programm mit dem Ziel, die Vorteile der Sensibilisierung für das Thema Informationssicherheit greifbar zu machen, ausgeführt und verwirklicht werden kann.

Rückmeldungen der an einem Sensibilisierungsprogramm beteiligten Nutzer lassen sich mit Feedback-Formularen einholen. Außerdem sollten die Nutzer dazu angehalten werden, im Hinblick auf die Informationssicherheit ungewöhnliche und verdächtige Aktivitäten möglichst umgehend zu melden. Beide Formulare geben Aufschluss darüber, inwieweit sich Verhalten, Einstellungen und Gewohnheiten der Nutzer aufgrund der Sensibilisierungsmaßnahmen geändert haben.

Muster für ein Feedback-Formular sowie für ein Formular zur Meldung von Vorfällen finden sich in den Anhängen X und XI.

Effizient kommunizieren

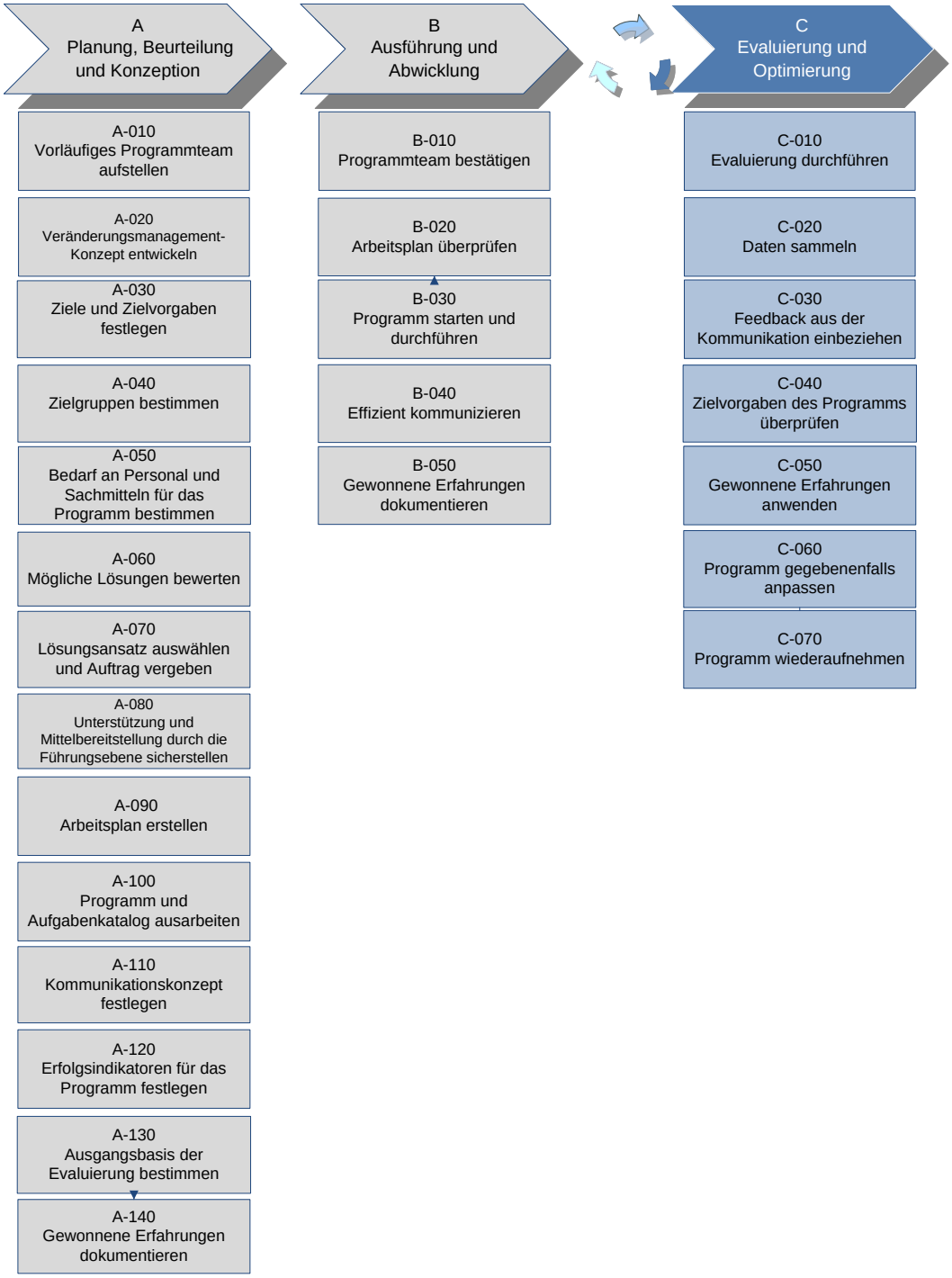
Sensibilisierung lässt sich nur durch Kommunikation mit den ausgewählten Zielgruppen erreichen. Damit ist nun der Zeitpunkt für die Umsetzung des Kommunikationsplans gekommen. Genauso wichtig ist das Einholen von Feedback über die Kommunikation zu dem Programm. Das Feedback vermittelt wertvolle Informationen, die für die nachfolgende Kommunikation von Nutzen sein können.

Gewonnene Erfahrungen dokumentieren

Nach Programmstart und Beginn der Durchführung müssen auch in dieser zweiten Phase die gewonnenen Erfahrungen dokumentiert werden. Hierzu wird das zum Ende von Phase I durchlaufene Verfahren wiederholt. Es ist sicherlich interessant, die Entwicklung des Programms über den zurückliegenden Zeitraum hinweg aus dieser Erfahrungsperspektive zu betrachten.

Aus vorangegangenen und ständig neu hinzukommenden Erfahrungen lernen, die Fähigkeit zur Veränderung ausbauen und Erfolge würdigen.

Phase III – Evaluierung und Optimierung



Evaluierung durchführen

Wie bereits in Phase I festgestellt, lässt sich messen, wie effektiv ein Sensibilisierungsprogramm ist und ob durch das Programm die Informationssicherheit verbessert wurde – auch wenn dies gelegentlich in Zweifel gezogen wird.
Die vor Programmbeginn ermittelte Ausgangsbasis vermittelt ein Bild von der Ausgangslage in den Zielgruppen. Anhand von Follow-up-Fragebogen und Mehrthemenbefragungen können Fortschritte bei der Sensibilisierung verfolgt werden und es lässt sich feststellen, wie gut die vermittelten Informationen im Bewusstsein der Nutzer verankert sind.

Eine unlängst von der ENISA durchgeführte Studie ergab, dass die Wirksamkeit von Initiativen zur Sensibilisierung für Informationssicherheit mit einer Vielzahl unterschiedlicher Methoden gemessen wird.([30]) Für die Organisationen ist es offenbar sehr schwierig, wirksame quantitative Messgrößen zu definieren. Demzufolge besteht auch keine Einigkeit darüber, welches nun die wirksamsten Maßnahmen sind. Im Idealfall würden die Organisationen gerne die tatsächlichen Veränderungen im Mitarbeiterverhalten messen können, die sich aus den Sensibilisierungsmaßnahmen ergeben.

Legende

How do you measure …	Wie messen Sie das Niveau des Bewusstseins für Informationssicherheit in Ihrer Organisation?
Results of audits …	Ergebnisse von Audits (durch interne oder externe Prüfer)
Number of security …	Anzahl der Sicherheitsvorfälle durch menschliches Fehlverhalten

([30]) ENISA, *Sensibilisierungsmaßnahmen zur Informationssicherheit: Die übliche Praxis und die Erfolgsmessung*, 2007, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/kpi/measuring_aw_de.pdf

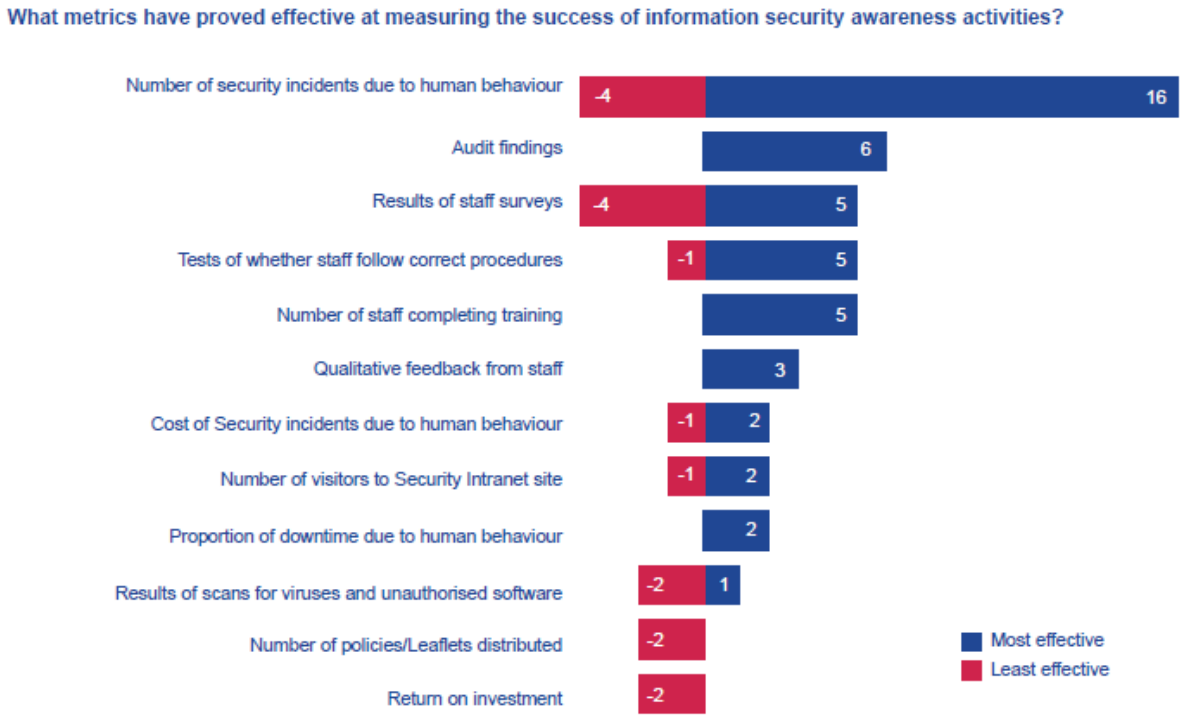
The root causes …	Hauptursachen der schwerwiegendsten Vorfälle
Proportion of security …	Anteil der Sicherheitsvorfälle durch menschliches Fehlverhalten
Number of staff …	Anzahl der Mitarbeiter, die erfolgreich an Sensibilisierungsschulungen teilgenommen haben
Results of staff …	Ergebnisse der Sicherheitserhebungen unter Mitarbeitern
Results of scans …	Ergebnisse der Suche nach Viren und nicht genehmigter Software
Qualitative feedback …	Qualitative Rückmeldungen von Zielgruppen oder Mitarbeitern
Cost of security incidents …	Kosten der Sicherheitsvorfälle durch menschliches Fehlverhalten
Proportion of downtime …	Anteil der Ausfallzeiten durch menschliches Fehlverhalten
Testing whether staff …	Tests, ob die Mitarbeiter die Vorgehensweisen korrekt einhalten
Number of visitors …	Anzahl der Aufrufe der Intranetseite zum Thema Sicherheit
Results of periodic …	Ergebnisse regelmäßiger Selbstbewertungen durch die Führungsebene
Proportion of purchases …	Anteil der Erwerbungen, die unter Berücksichtigung der Sicherheit getätigt wurden
Distribution of security policy …	Verbreitung von Informationen über Sicherheitsvorschriften oder Broschüren

Die beliebteste Informationsquelle über das tatsächliche Verhalten ist das (interne oder externe) Audit. Als Grund für die Verlässlichkeit der Auditberichte als Informationsquelle wird der objektive und systematische Ansatz der Prüfer angesehen.

Viele Organisationen verwenden als Messgröße ihre Erfahrung mit Sicherheitsvorfällen, und hier insbesondere die Anzahl der Vorfälle, die durch menschliches Fehlverhalten ausgelöst wurden, sowie die Analyse der Hauptursachen der schwerwiegendsten Vorfälle. Andere Organisationen hingegen verzichten auf Statistiken über Sicherheitsvorfälle als Maß für das Sicherheitsbewusstsein, da hier zahlreiche weitere Faktoren hineinspielen. Manche Organisationen nehmen daher Fragen zum Sicherheitsbewusstsein in Mitarbeiterbefragungen auf, wobei das Bewusstseinsniveau vor und nach der Initiative verglichen wird. Zum Teil wird jedoch auf Schwierigkeiten aufgrund der Komplexität der Erhebung und Verarbeitung der Daten hingewiesen. Auf diesem Gebiet müssen sich bewährte Verfahrensweisen eindeutig erst noch entwickeln.

Manche Parameter werden verwendet, weil sie Einblicke in das tatsächliche Verhalten vermitteln (z. B. Scans oder Tests). Andere werden angewendet, weil sie bei der Führungsebene, die die Sensibilisierungsprogramme finanziert und unterstützt, Anklang finden (z. B. Kosten der Vorfälle). BERR-Berichten zufolge geben die Unternehmen im Vereinigten Königreich für die Wiederherstellung der Sicherheit nach den schwerwiegendsten Vorfällen zwischen 1 000 und 2 000 GBP aus.([31])

([31]) BERR, *2008 Information security breaches survey*, 2008, im Internet abrufbar unter http://www.security-survey.gov.uk



Legende

What metrics have proved effective …	Welche Messgrößen haben sich bei der Erfolgsmessung von Maßnahmen zur Sensibilisierung für Informationssicherheit als wirksam erwiesen?
Number of security incidents …	Anzahl der Sicherheitsvorfälle durch menschliches Fehlverhalten
Audit findings	Ergebnisse eines Audit
Results of staff surveys	Ergebnisse von Mitarbeiterbefragungen
Tests of whether …	Tests, ob die Mitarbeiter die Vorgehensweisen korrekt einhalten
Number of staff completing …	Anzahl der Mitarbeiter, die Schulungen abgeschlossen haben
Qualitative feedback …	Qualitative Rückmeldungen von Mitarbeitern
Cost of Security incidents …	Kosten der Sicherheitsvorfälle durch menschliches Fehlverhalten
Number of visitors …	Anzahl der Aufrufe der Intranetseite zum Thema Sicherheit
Proportion of downtime …	Anteil der Ausfallzeiten durch menschliches Fehlverhalten
Results of scans …	Ergebnisse der Suche nach Viren und nicht genehmigter Software
Number of policies …	Anzahl der verteilten Informationen zu Vorschriften/Broschüren
Return on investment	Rentabilität
Most effective	Am wirksamsten
Least effective	Am wenigsten wirksam

Viele Organisationen hatten in der Vergangenheit Schwierigkeiten bei der Einführung wirksamer quantitativer Maßnahmen, wie z. B.:

- ✓ Probleme hinsichtlich Qualität und Vergleichbarkeit
- ✓ Relevanz der Messgrößen
- ✓ Verfügbarkeit bestimmter Indikatoren
- ✓ Gewichtung und Verarbeitung der Daten

Diese gängigen Probleme lassen sich vermeiden, wenn bereits im Vorfeld darauf geachtet wird. Ein möglichst einfacher Ansatz ist meist auch kostengünstig. Jede Organisation muss für ihr Umfeld die geeignete Methode finden – eine einheitliche Lösung, die in jedem Fall passt, gibt es nicht.

Nur durch eine ausgewogene Zusammenstellung der Messgrößen lässt sich wirklich Aufschluss über die Wirksamkeit von Sensibilisierungsprogrammen gewinnen. Und nur dann sind die betreffenden Organisationen in der Lage, ihre Programme so zu ändern, dass nicht nur die Vorschriften eingehalten werden, sondern dass sie wirklichen betrieblichen Nutzen daraus ziehen.

Den Erfolg des Programms messen

Im Allgemeinen wird das Sicherheitsbewusstsein anhand von vier Kategorien gemessen:

- ✓ Prozessverbesserung
- ✓ Widerstandsfähigkeit gegenüber Angriffen
- ✓ Effizienz und Effektivität
- ✓ interne Schutzmaßnahmen

Nachfolgend eine Beschreibung dieser Kategorien.

Prozessverbesserung

In dieser Kategorie geht es um die Entwicklung, Verbreitung und Anwendung von empfohlenen Sicherheitsleitlinien und Schulungsmaßnahmen zur Sensibilisierung. Bei der Evaluierung werden u. a. folgende Fragen gestellt:

- ✓ Wurden von der Behörde oder öffentlich-privaten Initiative empfohlene Sicherheitsleitlinien für die allgemeine Öffentlichkeit entwickelt? Sind diese Leitlinien gut verständlich und einprägsam formuliert? (Erwartete Antwort: Ja)
  Für KMU: Wurde eine allgemein

Internationale Geschäftsbank – Messungen sind für die Fokussierung der Maßnahmen wichtig

Eine große Geschäftsbank verfügt über ein zentrales Team für Informationssicherheit. Dieses Team trägt die Verantwortung für die weltweite Durchführung von Schulungsmaßnahmen zur Sensibilisierung. Sein Ziel ist die Vermittlung von Kernbotschaften über die Sicherheit an eine große Zielgruppe an verschiedenen Standorten. Außerdem sollen bestimmte Botschaften an kleinere Mitarbeitergruppen vermittelt werden, die wichtige Funktionen im System- oder Sicherheitsbereich ausüben.

Eine große Herausforderung für die Bank war die Messung des Sensibilisierungsgrads und der Wirksamkeit ihrer Sensibilisierungsprogramme. Im Idealfall sollten die Änderungen im Verhalten der Mitarbeiter gemessen werden, wobei eine quantitative Bewertung hier mit gewissen Schwierigkeiten verbunden ist. Da Messungen jedoch für die gezielte Ausrichtung der Schulungen auf die Schwachstellen eine wichtige Rolle spielen, hat die Bank in Analysen zur Ermittlung praktischer Messgrößen und Schlüsselleistungsindikatoren investiert.

Besonders der Einsatz von computerunterstützten Lernmethoden hat sich bewährt. Eine zentralisierte Bibliothek zu computerunterstützten Lernmethoden enthält Schulungskurse und erfasst die Testergebnisse von automatisierten Mitarbeitertests. Alle neuen Mitarbeiter müssen im Rahmen ihrer Einarbeitung an diesen Schulungen teilnehmen. Die Schulungsinhalte werden regelmäßig aktualisiert und müssen von allen Mitarbeitern durchgearbeitet werden. In Berichten werden der Stand der Durcharbeitung der Schulungsmaterialien sowie die Testergebnisse analysiert, das zentrale Team überwacht die Ergebnisse und reagiert auf wichtige Trends.

Passwortanalysen sind eine gute quantitative Messgröße für Einstellung und Verhalten der Mitarbeiter. Die Bank setzt regelmäßig eine Software ein, die die Passwortdateien der wichtigsten Systeme durchsucht und die Sicherheit der einzelnen Passwörter analysiert. Die Zahl der Mitarbeiter, die leicht nachzuvollziehende Passwörter verwendet, ist einer der wichtigsten Indikatoren für das Sicherheitsbewusstsein.

Als wirksame Techniken haben sich auch simulierte Phishing-E-Mails und Wettbewerbe erwiesen. Dadurch werden die Mitarbeiter angeregt, darüber nachzudenken, warum sie die Sicherheitsvorgaben erfüllen sollen. Zudem liefern sie nützliche Statistiken für die Trendanalyse.

In Kürze soll eine neue Umfrage durchgeführt werden, um das Sicherheitsbewusstsein und das Sicherheitsverhalten in der Bank zu messen. Hierzu wird ein unabhängiger Dritter eine nach dem Zufallsprinzip ausgewählte Stichprobe der Mitarbeiter befragen. Die Bank kann damit aus den Erhebungsergebnissen statistisch aussagekräftige Rückschlüsse für alle ihre Geschäftsfelder ziehen.

Zur Bewertung des Sicherheitsbewusstseins überwachte die Bank zunächst nur die Sicherheitsvorfälle. Eine Analyse der Hauptursachen ergab jedoch, dass für jeden Vorfall eine Vielzahl verschiedener Faktoren verantwortlich ist und die Zahl der Vorfälle allein das Sicherheitsbewusstsein nicht angemessen widerspiegelt. Hinzu kommt, dass Sicherheitsvorfälle so selten vorkommen, dass eine Trendanalyse nicht aussagekräftig ist. Aus diesen Gründen werden Vorfallstatistiken nicht mehr zur Messung des Sicherheitsbewusstseins verwendet.

gültige Sicherheitspolitik für das gesamte Unternehmen entwickelt? Ist diese gut verständlich und einprägsam formuliert? (Erwartete Antwort: Ja)

- ✓ Steht hinter den empfohlenen Sicherheitsleitlinien eine zuständige Behörde? Wird die Initiative angemessen unterstützt? (Erwartete Antwort: Ja)
  Für KMU: Steht die Unternehmensleitung hinter der allgemein gültigen Sicherheitspolitik? (Erwartete Antwort: Ja)
- ✓ Wie vielen der Befragten (in Prozent) ist bekannt, dass empfohlene Sicherheitsleitlinien existieren? Wie viele haben sie bereits gesehen oder gelesen? (Erwartete Veränderung: Anstieg)
  Für KMU: Wie hoch ist der prozentuale Anteil der KMU-Mitarbeiter, denen bekannt ist, dass eine Sicherheitspolitik existiert? Wie viele haben sie bereits gelesen? (Erwartete Veränderung: Anstieg)
- ✓ Wie viele der Befragten (in Prozent) glauben, dass sie die empfohlenen Sicherheitsleitlinien verstanden haben? (Erwartete Veränderung: Anstieg)
  Für KMU: Wie viele der Mitarbeiter (in Prozent) haben durch automatisierte Tests oder andere Prozesse nachgewiesen, dass sie die Sicherheitspolitik verstanden haben? (Erwartete Veränderung: Anstieg)
- ✓ Wie viele der Befragten (in Prozent) wissen, wie bei einem sicherheitsrelevanten Vorfall vorzugehen ist oder an wen sie sich in einem solchen Fall wenden können? (Erwartete Veränderung: Anstieg)
  Für KMU: Wie viele der Mitarbeiter (in Prozent) wissen, an wen sie sich bei einem sicherheitsrelevanten Vorfall wenden oder wie sie sich verhalten sollen? (Erwartete Veränderung: Anstieg)
- ✓ Wenn eine neue Bedrohung erkannt wurde – wie lange dauert es durchschnittlich, bis die Behörde/Initiative flächendeckend eine Warnung per E-Mail versendet oder Warnungen auf häufig aufgerufenen Websites veröffentlicht? (Erwartete Veränderung: Rückgang)
  Für KMU: Wenn eine neue Bedrohung erkannt wurde – wie lange dauert es durchschnittlich, bis unternehmensweit eine Warnung per E-Mail versendet wird? (Erwartete Veränderung: Rückgang)
- ✓ Wurde ein Schulungsprogramm zur Sensibilisierung entwickelt und eingeführt? (Erwartete Antwort: Ja)
  Für KMU: Wurde ein Schulungsprogramm zur Sensibilisierung entwickelt? (Erwartete Antwort: Ja)
- ✓ Wie viele Personen (in Prozent der Befragten) haben diese Schulung absolviert? (Erwartete Veränderung: Anstieg)
  Für KMU: Wie viele Mitarbeiter (in Prozent) haben diese Schulung absolviert? (Erwartete Veränderung: Anstieg)
- ✓ Wie oft wird der Inhalt des Schulungsprogramms aktualisiert? (Erwartete Veränderung: Anstieg)
  Für KMU: In welchen durchschnittlichen Zeitabständen nehmen die Mitarbeiter an einer solchen Schulung teil? (Erwartete Veränderung: Rückgang)
  Für KMU: Wurden wegen Nichteinhaltung der Sicherheitspolitik Kündigungen ausgesprochen? Wie viele? (Erwartete Veränderung: Rückgang)
  Für KMU: Gibt es ein Programm für interne und externe Sicherheitsaudits? (Erwartete Antwort: Ja)
  Für KMU: Wurde in den internen und externen Sicherheitsaudits eine verbesserte Einhaltung der Sicherheitspolitik nachgewiesen? (Erwartete Antwort: Ja)

Widerstandsfähigkeit gegenüber Angriffen

Diese Kategorie betrifft das Erkennen von sicherheitsrelevanten Vorfällen und die Widerstandsfähigkeit gegenüber Angriffen. Bei der Evaluierung werden beispielsweise folgende Fragen gestellt:([32])

- ✓ Inwieweit sind die Mitarbeiter in der Lage, Angriffe zu erkennen?
- ✓ Inwieweit werden Angriffe von den Mitarbeitern nicht als solche erkannt?
- ✓ Wie viele Personen (in Prozent der Befragten) erkennen im Test ein Szenario mit einem sicherheitsrelevanten Vorfall? (Erwartete Veränderung: Anstieg)
- ✓ Von wie vielen Personen (in Prozent der Befragten) wurde im Test der sicherheitsrelevante Vorfall nicht erkannt? (Erwartete Veränderung: Rückgang)
- ✓ Wie viele Personen (in Prozent der Befragten) gaben im Test ihr Passwort preis? (Erwartete Veränderung: Rückgang)
  Für KMU: Wie viele IT-Administratoren oder Helpdesk-Mitarbeiter (in Prozent) reagierten nicht auf einen unzulässigen Passwortänderungsversuch? (Erwartete Veränderung: Rückgang)
- ✓ Von wie vielen Nutzern (in Prozent) wurde ein „Testvirus" aktiviert? (Erwartete Veränderung: Rückgang)

Effizienz und Effektivität

In dieser Kategorie geht es um Effizienz und Effektivität mit Blick auf sicherheitsrelevante Vorfälle. Bei der Evaluierung werden beispielsweise folgende Fragen gestellt:

- ✓ Bei welchem Anteil (in Prozent) der von den Befragten erlebten sicherheitsrelevanten Vorfälle war die Hauptursache menschliches Fehlverhalten? (Erwartete Veränderung: Rückgang)
- ✓ Welcher Anteil (in Prozent) der Ausfallzeiten war auf sicherheitsrelevante Vorfälle zurückzuführen? (Erwartete Veränderung: Rückgang)
  Für KMU: Wie hoch sind die Ausgaben des Unternehmens für Sensibilisierungsmaßnahmen als Anteil (in Prozent) an den Sicherheitsausgaben und/oder des Unternehmensgewinns? (Erwartete Veränderung: Rückgang)

Interne Schutzmaßnahmen

Bei dieser Kategorie geht es darum, wie gut der einzelne Nutzer gegen mögliche Gefahren geschützt ist. Bei der Evaluierung werden beispielsweise folgende Fragen gestellt:

- ✓ Bei welchem Anteil (in Prozent) der von den Befragten getätigten Software- und Hardwarekäufe spielten Sicherheitsaspekte eine Rolle? (Erwartete Veränderung: Anstieg)
  Für KMU: Welcher Anteil (in Prozent) der Software, Geschäftspartner und Lieferanten des Unternehmens wurde einer Sicherheitsüberprüfung (einschließlich Awareness-Test) unterzogen? (Erwartete Veränderung: Anstieg)
- ✓ Welcher Anteil (in Prozent) der wichtigen Daten der Befragten ist „sehr gut" geschützt? (Erwartete Veränderung: Anstieg)
  Für KMU: Welcher Anteil (in Prozent) der wichtigen Daten des Unternehmens ist „sehr gut" geschützt – einschließlich Sensibilisierungsmaßnahmen für Datenmanager, Administratoren usw.? (Erwartete Veränderung: Anstieg)

([32]) ENISA, *Sensibilisierungsmaßnahmen zur Informationssicherheit: Die übliche Praxis und die Erfolgsmessung*, 2007, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/kpi/measuring_aw_de.pdf

- ✓ Welcher Anteil (in Prozent) der wichtigen Daten der Befragten ist nicht entsprechend den empfohlenen Leitlinien geschützt? (Erwartete Veränderung: Rückgang)
  Für KMU: Welcher Anteil (in Prozent) der wichtigen Daten des Unternehmens ist nicht entsprechend den Sicherheitsstandards des Unternehmens geschützt? (Erwartete Veränderung: Rückgang)
- ✓ Auf welchem Anteil der Systeme der Befragten war bösartige Software oder Spyware installiert? (Erwartete Veränderung: Rückgang)
- ✓ Auf welchem Anteil der Systeme der Befragten waren Software-Raubkopien installiert? (Erwartete Veränderung: Rückgang)

Daten sammeln

Für die Sammlung von Daten, die für die Messung der Leistungsfähigkeit von Sensibilisierungsinitiativen herangezogen werden, wird empfohlen, eine Kombination von quantitativen und qualitativen Information zu erfassen. Die Daten sollten fortlaufend erfasst werden (da die Messung der Leistungsfähigkeit einer Initiative und die Überwachung ihrer Wirksamkeit sowohl während als auch nach der Durchführung der Initiative erfolgen sollten). Idealerweise werden die Daten mittels automatisierter Prozesse erfasst.

Für die Erhebung von Daten stehen unter anderem folgende Methoden zur Auswahl: Fragebogen, Website-Statistiken, allgemeine Beobachtungen, Statistiken aus Datenzentren, Schwerpunktgruppen, Daten von Callcentern/Hotlines, Zahl der Meldungen an den IT-Support, Presseberichte, Newsletter, Pressemitteilungen, Zahl der Abonnenten von Online-Diensten, Zahl der Personen, die an einer Schulung teilgenommen haben.

Feedback aus der Kommunikation einbeziehen

Das Feedback, das im Rahmen der Kommunikation zu dem Programm eingeholt wurde, sollte unter dem Aspekt überprüft werden, wie sich die Kommunikation künftig noch besser und wirkungsvoller gestalten lässt. Die dabei gewonnenen Informationen sollten dann mit den Messergebnissen aus der Evaluierung zusammengeführt werden.

Zielvorgaben des Programms überprüfen

Die Zielvorgaben des Programms müssen vor dem Hintergrund der Effektivitätsresultate überprüft werden. Was hat das Team erreicht? Wurde der angestrebte Nutzen erreicht? Wenn ja, dann sollte dies auch gebührend gewürdigt werden. Wenn nicht, wie lassen sich die gewünschten Ergebnisse erzielen? Oder müssen die Zielvorgaben geändert werden? Bei einer Überprüfung der Zielvorgaben kann eine gründliche Bewertung vorgenommen werden.

Gewonnene Erfahrungen anwenden

Die Erfahrungen aus dem Sensibilisierungsprogramm können nun

Behörde – Gewonnene Erfahrungen umsetzen

Eine Behörde erläutert, weshalb die Dokumentation gewonnener Erfahrungen im Hinblick auf die Effektivität und den Erfolg künftiger Programme zunehmend an Bedeutung gewinnt. In der Behörde soll damit sichergestellt werden, dass alle Erfahrungen der Vergangenheit – die positiven ebenso wie die weniger positiven – in die Planung künftiger Sensibilisierungsinitiativen einfließen.

Als besonders hilfreich hat sich dabei die Einschaltung eines externen Unternehmens erwiesen, das in speziellen Teamsitzungen Rückmeldungen aus dem Programmteam sammelt. An diesen Sitzungen nimmt das gesamte Programmteam teil. Das externe Unternehmen unterstützt die Behörde dabei, die so gewonnenen Erkenntnisse in die künftige Planung einzubeziehen.

ausgewertet werden. Welche Erfahrungen können dazu genutzt werden, das Programm künftig noch effektiver und erfolgreicher zu gestalten? Der Hauptschwerpunkt liegt dabei darauf, aus den – positiven und auch weniger positiven – Erfahrungen der Vergangenheit zu lernen und das Gelernte in die Praxis umzusetzen.

Programm gegebenenfalls anpassen

Die seit Programmbeginn gewonnenen Erfahrungen vermitteln das Wissen und die notwendigen Erkenntnisse für eine Anpassung des Programms, um es künftig noch erfolgreicher zu gestalten. Die notwendigen Anpassungsmaßnahmen können durchweg jede Aktivität und jeden Aufgabenbereich im Rahmen des Programms betreffen. Dabei geht es darum, Anpassungen vorzunehmen, ohne dabei die Zielvorgaben und Zielsetzungen des Programms aus den Augen zu verlieren.

Programm wiederaufnehmen

Nachdem anhand der bislang gewonnenen Erfahrungen Anpassungen am Programm vorgenommen wurden, steht nunmehr die Wiederaufnahme des Programms an, womit Phase II abgeschlossen wäre. Dieser Zeitpunkt bietet eine ideale Gelegenheit, weitere Themen zu vertiefen oder sich intensiver mit Problemstellungen zu befassen, die bereits zu einem früheren Zeitpunkt angesprochen wurden.

Laufend aus den gewonnenen Erfahrungen lernen, die Fähigkeit zur Veränderung stärken und Erfolge würdigen

TEIL 3: HINDERNISSE AUF DEM WEG ZUM ERFOLG ÜBERWINDEN

Erfolgshindernisse

Die Durchführung eines erfolgreichen Programms zur Sensibilisierung für Informationssicherheit kann sich als schwierige Aufgabe erweisen. Selbst bei sorgfältig geplanten Programmen können schwer zu überwindende Hindernisse auftreten. Wenn man sich allerdings bereits im Vorfeld mit den am häufigsten vorkommenden Hindernissen befasst, lassen sich diese bereits in der Planungs- und Durchführungsphase ausschalten.

	Beschreibung
Einführung einer neuen Technologie	Die Einführung einer neuen Technologie verlangt den Nutzern zumeist eine gewisse Verhaltensänderung oder die Auseinandersetzung mit neuen Konzepten ab. Dies allein stellt an sich kein Problem dar, doch schreitet gelegentlich die Technologie schneller als das Sensibilisierungsprogramm oder losgelöst von diesem voran. Es kann vorkommen, dass das Sensibilisierungsteam die Möglichkeiten, die eine neue Technologie bietet, noch nicht kennt oder sich nicht genügend damit auskennt. Deshalb ist es wichtig, dass im Rahmen des Sensibilisierungsprogramms auf die interne Kommunikation Wert gelegt und dafür gesorgt wird, dass eine Kommunikationsstrategie für Not- oder Krisenfälle erstellt wird.
Mangelnde Zielgruppenorientierung	Bei manchen Sensibilisierungsprogrammen wird versäumt, das Zielpublikum in geeigneter Weise zu untergliedern und die Zielgruppen mit adäquaten Botschaften anzusprechen. Dies führt schlimmstenfalls dazu, dass die Botschaften ignoriert werden. IT-Nutzer erhalten Tag für Tag Hunderte von Botschaften aus unterschiedlichsten Quellen, daher ist es entscheidend, das Zielpublikum zu untergliedern und dafür Sorge zu tragen, dass die einzelnen Zielgruppen nur die auf sie zugeschnittenen Botschaften erhalten. Eine Einheitsstrategie ist zwar möglicherweise einfacher zu entwickeln und umzusetzen, führt jedoch nicht zum Erfolg.
Informationsüberflutung	Informationsüberflutung ist ein häufig vorkommender Fehler. In der Regel gibt es beim Zielpublikum eine Schwelle, über die hinaus keine Informationen mehr aufgenommen werden. Wenn die Nutzer ständig mit Botschaften „bombardiert" werden, verlieren sie das Interesse. Auch wenn das Zielpublikum sorgsam untergliedert wurde und nur mit adäquaten Botschaften angesprochen wird, wird ein „Zuviel" an Information einfach nicht mehr wahrgenommen. Ein Sensibilisierungsprogramm muss nicht kurzfristig angelegt sein. Nehmen Sie sich die Zeit, auf die Bedürfnisse der Zielgruppe einzugehen und das richtige Maß zu finden.
Organisatorische Mängel	Bei Sensibilisierungsprogrammen wird häufig der Fehler gemacht, dass keine durchgängig einheitlichen Prozesse und Strategien für die Vermittlung der Botschaft entwickelt werden. Fehlt die Einheitlichkeit bei Konzept, Themenstellung und Umsetzung, fällt es dem Nutzer schwer, sich auf das Programm einzulassen, und er weiß nicht, was ihn erwartet. Entscheidend ist die Konsistenz der Kommunikation. Sie trägt auch dazu bei, dem Programm eine Identität zu verleihen und eine Beziehung zur Zielgruppe aufzubauen.
Mangelndes Follow-up	Nicht selten werden Sensibilisierungsprogramme mit großem Enthusiasmus in Angriff genommen, nur um dann letztlich im Sand zu verlaufen. Bei vielen Programmen gelingt es nicht, einen regelmäßigen Kommunikationszyklus zu etablieren und aufrechtzuerhalten. Die regelmäßige Kommunikation ist wichtig, um den Nutzern regelmäßig die

	wichtigen Botschaften ins Gedächtnis zu rufen. Häufig wird auch versäumt, bei der Zielgruppe nachzufassen und Feedback einzufordern. Auf das Zielpublikum zu hören und das Programm an dessen Bedürfnisse anzupassen, ist ein wichtiger Faktor.
Die Botschaft muss dort ansetzen, wo sich Wirkung erzielen lässt	Es ist manchmal ziemlich schwierig, die richtige Botschaft dem richtigen Zielpublikum zu vermitteln. Ganz besonders trifft dies bei einem großen Adressatenkreis zu. Ein Beispiel: Selbst wenn von einer Gemeindeverwaltung bereits eine durchdachte Kommunikationsstrategie mit einem genau konzipierten Prozess für die zielgerichtete Kommunikation ausgearbeitet wurde, kann es sich dennoch als ausgesprochen schwierig erweisen, die richtige Botschaft dem richtigen Publikum zu vermitteln. Nach individuellen Kriterien zusammengestellte E-Mail-Gruppen können hier hilfreich sein, lösen das Problem aber nicht vollständig. Es kann auch vorkommen, dass ein bestimmtes Zielpublikum ermittelt wurde, es jedoch Probleme bereitet genau festzustellen, wer zu diesem Zielpublikum gehört. Ein Beispiel hierfür sind Botschaften, mit denen eine bestimmte Zielgruppe angesprochen werden soll. Wenn beispielsweise Eltern anhand der Schulanmeldung ihrer Kinder ermittelt wurden, kann es durchaus sein, dass die Liste der Eltern nicht vollständig ist, weil einzelne Kinder beim anderen Elternteil leben. Die Herausforderung besteht nun darin, eine Liste aufzustellen und zu pflegen, die gewährleistet, dass immer alle Eltern alle sie betreffenden Mitteilungen erhalten. Das ist nicht einfach.
Fehlende Ressourcen	Ursache hierfür ist in der Regel mangelnde Unterstützung durch die Führungsebene. Fehlt diese Unterstützung, ist es schwierig, angemessene Mittel zu beschaffen, und ohne angemessene Mittelausstattung ist die Reichweite eines Sensibilisierungsprogramms, was seinen Erfolg anbelangt, begrenzt.
Keine ausreichende Begründung	Bei vielen Sensibilisierungsprogrammen wird versäumt, die Nutzer hinreichend darüber aufzuklären, weshalb Sicherheit ein wichtiges Thema ist. Alle übrigen Aspekte werden bedacht, aber unglücklicherweise fehlt genau die Information, die die Nutzer am ehesten zu einer Verhaltensänderung veranlassen würde. Nutzer, die darüber aufgeklärt wurden, weshalb bestimmte Verhaltensweisen eine Gefahr darstellen, machen sich das Thema eher zu eigen und ändern ihr Verhalten entsprechend. Werden beispielsweise Handlungsempfehlungen für einen neuen Passwortprozess ausgegeben, der striktere Vorschriften für den Aufbau des Passworts vorsieht, werden die meisten Nutzer in dem neuen Prozess nur eine zusätzliche Unannehmlichkeit sehen. Wenn aber auch vermittelt wird, wie Passwörter geknackt und missbraucht werden und welche Folgen dies haben kann, dann sind die Aussichten, dass die Nutzer die neuen Handlungsempfehlungen befolgen, größer.
Social Engineering	„Social Engineering" oder „soziale Instrumentalisierung" hat nicht zwangsläufig Auswirkungen auf die Durchführung eines Sensibilisierungsprogramms, kann jedoch den Erfolg beeinträchtigen. Das Thema ist deshalb wichtig, weil es genau auf die „menschliche Verbindung" abzielt, die durch ein Sensibilisierungsprogramm gestärkt werden soll. Als „Social Engineering" bezeichnet man die Technik, die naturgegebene menschliche Neigung, anderen zu vertrauen und helfen zu wollen, dazu zu nutzen, sich Informationen zu verschaffen, an die auf anderem Wege nur schwer heranzukommen ist. Die meisten Menschen sind überzeugt, dass niemand auf die Idee kommen würde, die Öffentlichkeit bewusst zu täuschen oder zu manipulieren, doch

	tatsächlich zählt Social Engineering zu den gebräuchlichsten Angriffsformen. Angreifer wählen diese Methode gerne, weil sie so überraschend einfach anzuwenden ist und verhältnismäßig wenig Zeitaufwand erfordert. Weshalb sollte sich ein Angreifer damit aufhalten, mühsam ein Passwort zu knacken, wenn sich das Ziel viel einfacher erreichen lässt, indem er vorgibt, ein Helpdesk-Mitarbeiter einer Bank oder einer anderen vertrauenswürdigen Einrichtung zu sein, und einen leichtgläubigen Nutzer dazu veranlasst, ihm sicherheitsrelevante Informationen zu geben? Zu den gebräuchlichsten Methoden des Social Engineering zählen der Identitätswechsel (Impersonation), Einschmeicheln und Glaubhaftmachen einer Dringlichkeitssituation sowie die vermeintliche Autorisierung durch Dritte. Eine Aufklärungsstrategie, die sich gezielt mit diesem Themenbereich befasst, sollte dringend entwickelt und eingeführt werden. Leider ist jedoch – wie Granger, Steven und Berg, anerkannte Fachleute auf dem Gebiet der Informationssicherheit und des Social Engineering, anschaulich schildern – das Social Engineering eine Angriffsform, durch die sich selbst ausgesprochen sicherheitsbewusste Nutzer überlisten lassen.
Veränderung gewohnter Verhaltensmuster	In vielen Organisationen kümmert man sich erst im Nachhinein um Informationssicherheit. Weil Sicherheitsvorkehrungen nicht von Beginn an integriert werden, vergehen Wochen, Monate und manchmal sogar Jahre, in denen sich bei den Nutzern sicherheitsabträgliche Verhaltensweisen einschleichen. Dadurch wird die Einführung eines Sensibilisierungsprogramms zusätzlich erschwert. Die Nutzer müssen nicht nur über Sicherheitsfragen aufgeklärt werden, sondern sie müssen auch dabei unterstützt werden, schlechte Angewohnheiten abzulegen. Hinzu kommt, dass es den Nutzern dann schwerer fällt, den Wert von Sicherheitsmaßnahmen einzusehen. Aus ihrer Sicht ist auch ohne Informationssicherheit bisher alles bestens gelaufen. Neue Sicherheitsanforderungen werden als unnötige Veränderungen wahrgenommen, die den Nutzern das Leben schwer machen.
„Sicherheit ist Sache der IT-Abteilung – mich geht das nichts an …"	Viele Nutzer sind der Auffassung, dass Sicherheit alleine Sache der IT-Abteilung ist. Ihre eigene Rolle beschränken sie auf das absolute Minimum, das erforderlich ist, um den Arbeitsplatz nicht zu verlieren – ihre Rolle als Teil der Lösung sehen sie nicht. Die Einhaltung der Sicherheitsvorschriften ist hier zwar ein erster Schritt, aber sie könnten noch deutlich mehr zur Sicherheit beitragen. Es kommt daher darauf an, allen Nutzern klar zu machen, dass die IT-Abteilung Informationssicherheit nicht im Alleingang gewährleisten kann. So werden beispielsweise laut einer im Juni 2008 veröffentlichten Umfrage des Ponemon Institute alleine bei den großen und mittelgroßen Flughäfen in den USA jährlich fast 637 000 herrenlose Laptops registriert. Wie aus der Umfrage weiter hervorgeht, bleiben die meisten Laptops bei den Sicherheitskontrollen liegen. Bei 36 der größten US-Flughäfen werden pro Woche etwa 10 278 Laptops gefunden; 65 % dieser Geräte werden laut Umfrage von ihren Besitzern nicht abgeholt. Auf den mittelgroßen US-Flughäfen werden rund 2 000 Laptops gefunden, 69 % davon werden nicht abgeholt.([33]) In Europa werden in einem typischen Monat am Flughafen

([33]) Shah, Agam, „Laptops lost like hot cakes at US airports", *PC World*, 30. Juni 2008, im Internet abrufbar unter http://www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airports.html (zuletzt aufgerufen am 15. Juli 2008); US Research Ponemon Institute LLC, *Airport insecurity: The case of lost*

	London Heathrow bis zu 120 Laptops beim Fundbüro abgegeben. Rund 40 % aller abgegebenen Elektronikgeräte, der Großteil davon Mobiltelefone, werden nicht wieder abgeholt.([34])
Unzureichende Unterstützung durch das Management	Sich der Unterstützung des Managements zu versichern, gehört zu den Grundvoraussetzungen für die Durchführung eines Sensibilisierungsprogramms. Zugleich ist dies eine der anspruchsvollsten Aufgaben überhaupt. Wenn Botschaften zur Informationssicherheit wirksam sein sollen, müssen sie von der Führungsebene propagiert werden. Zwar zeigen sich Führungskräfte meist daran interessiert, Sicherheitsinitiativen zu unterstützen, die aktive Umsetzung ist jedoch eine ganz andere Sache. Grund hierfür ist, dass Führungskräfte eigene Aufgaben und Verantwortungsbereiche haben, für die sie zuständig sind. Ihr primäres Ziel muss sein, die Geschäftsziele zu verwirklichen, sodass es für sie oft schwierig ist, sich auch noch um das Thema Sicherheit zu kümmern – egal für wie wichtig sie selbst es halten.

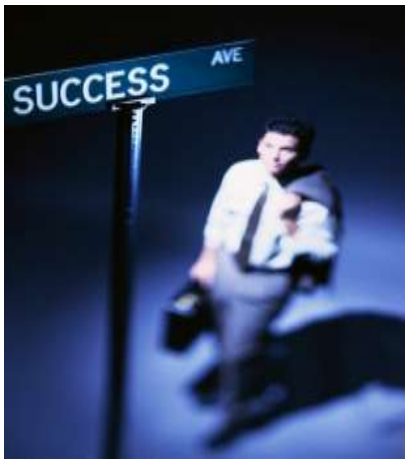
laptops, Executive summary, 2008, im Internet abrufbar unter http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf (zuletzt aufgerufen am 15. Juli 2008).

([34]) Dabbs, Alistair, „Where do all the missing laptops go?", *IT Week*, 18. September 2006, im Internet abrufbar unter http://www.itweek.co.uk/itweek/comment/2164474/missing-laptops (zuletzt aufgerufen am 22. Juli 2008).

Entscheidende Faktoren für den Erfolg

Zu den wichtigen Faktoren, die über den Erfolg eines Informationssicherheitsprogramms entscheiden, zählen unter anderem:

- ✓ Als Ausgangsbasis für die Durchführung oder die Wiederaufnahme eines Sensibilisierungsprogramms muss zunächst eine Bestandsaufnahme der Ist-Situation vorgenommen werden.
- ✓ Sensibilisierungsprogramme haben nur dann Aussicht auf Erfolg, wenn es gelingt, das Zielpublikum anzusprechen.
- ✓ Nutzen Sie NRO, Institutionen, Banken, Internetdiensteanbieter, Bibliotheken, örtliche Handelsverbände, Gemeindezentren, Computerläden, Volkshochschulen und Erwachsenenbildungsprogramme, Schulen und Eltern-Lehrer-Verbände für die Vermittlung der Botschaft.
- ✓ Wichtig ist, dass die Sensibilisierungskampagne öffentlichkeitswirksam in Szene gesetzt wird, denn durch eine möglichst große Zahl von Kontakten lässt sich die Wirkung der Kampagne vervielfachen.
- ✓ Setzen Sie im Bedarfsfall auf öffentlich-private Partnerschaft.



- ✓ Grundvoraussetzung für den Erfolg von Sensibilisierungsprogrammen ist, dass sie der Kultur der Organisation nicht zuwiderlaufen und dass sie von der Führungsebene unterstützt werden.
- ✓ Eine nachhaltige Unterstützung für Sensibilisierungsprogramme setzt voraus, dass nachgewiesen werden kann, dass die Bemühungen um Informationssicherheit Früchte tragen.

Der Erfolg – oder Misserfolg – von Initiativen zur Sensibilisierung für Informationssicherheit kann anhand der in diesem Leitfaden vorgestellten Messgrößen nachgewiesen werden.

Fazit

Die Bürger von heute sind sehr mobil und kommunizieren in zunehmendem Maße über das Internet. Die Folge: Sie benötigen zu jeder Zeit und an jedem Ort zuverlässige und sichere Kommunikationsverbindungen. Dieser neue Trend eröffnet den Nutzergemeinschaften Tausende neuer Möglichkeiten. Allerdings birgt diese rapide Ausweitung der Push- und Pull-Kommunikation auch Sicherheitsrisiken, und es ist Aufgabe von Behörden und Unternehmen, die damit einhergehenden Probleme zu lösen.

Jedes System ist nur so stark wie seine schwächste Komponente. Menschliche Fehler können selbst das ausgeklügeltste Informationssicherheitskonzept untergraben. Das Bewusstsein der Nutzer für die Risiken, aber auch für die zur Verfügung stehenden Schutzmaßnahmen bilden die vorderste Verteidigungslinie für die Sicherheit von Informationssystemen und -netzen.

Die ENISA hofft, privaten und öffentlichen Organisationen mit diesem Leitfaden ein wertvolles Hilfsmittel für die Vorbereitung und Durchführung von Initiativen und Programmen zur Sensibilisierung für Informationssicherheit an die Hand zu geben. Informationssicherheit zu schaffen ist eine enorme Aufgabe – spezifische Zielgruppen für das Thema zu sensibilisieren, ist ein wichtiger erster Schritt zur Bewältigung dieser Aufgabe.

Literaturverzeichnis

Ajzen, Icek und Fishbein, Martin, *Understanding attitudes and predicting social behaviour*, Prentice-Hall Inc., USA, 1980.

Ajzen, Icek, *Attidudes, Personality and behaviour*, Second edition, Open University Press, USA, 2005.

Basiliere, Pete, *Information breach highlights production print and mail vulnerabilities,* Gartner, 18. September 2007.

Bayan, Ruby, „Success strategies for security awareness", *TechRepublic*, 2004, im Internet abrufbar unter http://techrepublic.com.com/5100-10878_11-5193710.html# (zuletzt aufgerufen am 16. Juli 2008).

BERR, *2008 Information security breaches survey*, 2008, im Internet abrufbar unter http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

Center for Internet Security
http://www.cisecurity.org/resources.html

CERT Virtual Training Environment, im Internet abrufbar unter https://www.vte.cert.org/vtelibrary.html (zuletzt aufgerufen am 17. Juli 2008).

Cybersecurity Awareness Resource Library
http://www.educause.edu/CybersecurityAwarenessResourceLibrary/8762

Dabbs, Alistair, „Where do all the missing laptops go?", *IT Week*, 18. September 2006, im Internet abrufbar unter http://www.itweek.co.uk/itweek/comment/2164474/missing-laptops (zuletzt aufgerufen am 22. Juli 2008).

Deloitte, *Bringing IT into the boardroom — Implementing technology as a strategic resource for the board,* 2006, im Internet abrufbar unter http://www.deloitte.com/dtt/cda/doc/content/us_consulting_ti_bringingitbrdrm_201106%284%29.pdf

Deloitte, *2008 Survey on the IT-business balance*, 2008, im Internet abrufbar unter http://www.deloitte.com/dtt/cda/doc/content/IT%20Business%20Balance%20Report_2008_CMYK.pdf. (zuletzt aufgerufen am 21. Juli 2008).

ENISA, *Raising awareness in information security — Insight and guidance for Member States,* 2005, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cd_awareness_raising.pdf

ENISA, *Sensibilisierungsmaßnahmen zur Informationssicherheit: Die übliche Praxis und die Erfolgsmessung*, 2007, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/kpi/measuring_aw_de.pdf

ENISA, *Key facts and figures about the AR Community and its members*, 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/deliverables/ar_comm_key_facts.pdf

ENISA, *Sicherer Umgang mit USB-Speichersticks,* 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/publications/secure_usb_flash_drives_de.pdf

ENISA*, Sicheres Drucken,* 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/ENISA_secure_printing_de.pdf

ENISA*, Unterstützung und Mittelbereitstellung durch die Unternehmensleitung*, 2008, im Internet abrufbar unter http://www.enisa.europa.eu/doc/pdf/other/awareness/support_management_DE.pdf

Ford, Richard, „Disc listing foreign criminals lost for year‟ *The Times*, 20. Februar 2008, im Internet abrufbar unter http://www.timesonline.co.uk/tol/news/politics/article3399712.ece (zuletzt aufgerufen am 15. Juli 2008).

Getsafeonline
http://www.getsafeonline.org/

Girard, John und Litan, Avivah, *New data loss highlights problems with contractors and laws,* Gartner, 4. Februar 2008.

Heidt, Erik T., *Basics of the quick business case: How to champion your next information security initiative*, RSA Conference Europe 2007, 2007, im Internet abrufbar unter http://artofinfosec.com/22/art-of-info-sec-001-quick-business-case/ (zuletzt aufgerufen am 22. Juli 2008).

Herold, Rebecca, *Addressing the insider threat,* IT Compliance in Realtime, Realtime publishers, Mai 2008, Volume I, Number 3, im Internet abrufbar unter http://nexus.realtimepublishers.com/RTITC.htm (zuletzt aufgerufen am 31. Juli 2008).

Herold, Rebecca, *Information security and privacy awareness program*, Auerbach Publications, USA, 2005.

Hinson (Dr), Gary, „The true value of information security awareness‟, *Noticebored*, 2008, im Internet abrufbar unter http://www.noticebored.com/html/why_awareness_.html (zuletzt aufgerufen am 17. Juli 2008).

Housel, Thomas und Bell, Arthur H., *Measuring and managing knowledge*, McGraw-Hill international edition, Singapur, 2001.

Information Systems Security Association
http://www.issa.org/

Information Warfare Site, *Security awareness toolbox*, im Internet abrufbar unter http://www.iwar.org.uk/comsec/resources/sa-tools/ (zuletzt aufgerufen am 5. Juli 2008).

IT Governance Institute, *Information security governance: Guidance for boards of directors and executive management*, second edition, USA, 2006.

Jevans, Dave, *Privacy and identity theft,* IronKey, im Internet abrufbar unter http://blog.ironkey.com/?cat=9&paged=2 (zuletzt aufgerufen am 20. Mai 2008).

McMurchy, Neil*, Take these steps to develop successful BI business cases,* Gartner, 1. Februar 2008.

McMurchy, Neil, *Toolkit: Building the business intelligence business case — Identifying and calculating benefits,* Gartner, 25. April 2008.

National Cyber Security Alliance (NCSA)
http://www.staysafeonline.org/

NIST, *Information technology security training requirements: A role- and performance-based model*, NIST — SP 800-16, USA, 1998, im Internet abrufbar unter http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (zuletzt aufgerufen am 21. Juli 2008).

NIST, *Building an information technology security awareness program*, NIST — SP800-50, USA, 2003, im Internet abrufbar unter http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (zuletzt aufgerufen am 17. Juli 2008).

Noticebored, *Business case for an information security awareness program*, 2008, im Internet abrufbar unter http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (zuletzt aufgerufen am 17. Juli 2008).

OECD, *Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security,* DSTI/ICCP/REG(2003)5/REV1, Working Party on Information Security and Privacy, OECD, 2003, im Internet abrufbar unter http://www.oecd.org/dataoecd/23/11/31670189.pdf

Parmenter, David, *Key performance indicators – Developing, implementing and using winning KPIs*, John Wiley & Sons Inc., USA, 2007.

Rasmussen, Gideon, *Building a security awareness program — Addressing the threat from within*, im Internet abrufbar unter http://www.gideonrasmussen.com/article-01.html (zuletzt aufgerufen am 16. Juli 2008).

Roberts, John P., *Toolkit sample template: An effective business case,* Gartner, 11. Juli 2007.

SANS, *SANS InfoSec Reading Room — Security Awareness Section*, im Internet abrufbar unter http://www.sans.org/rr/whitepapers/awareness/ (zuletzt aufgerufen am 17. Juli 2008).

SANS, *The SANS security policy project*, im Internet abrufbar unter http://www.sans.org/resources/policies/ (zuletzt aufgerufen am 17. Juli 2008).

Shah, Agam, „Laptops lost like hot cakes at US airports", *PC World*, 30. Juni 2008, im Internet abrufbar unter http://www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airport.html (zuletzt aufgerufen am 15. Juli 2008).

US-CERT, *Cyber security tips*, im Internet abrufbar unter http://www.us-cert.gov/cas/tips/index.html (zuletzt aufgerufen am 17. Juli 2008).

US-CERT, *Home network security*, im Internet abrufbar unter http://www.us-cert.gov/reading_room/home-network-security/ (zuletzt aufgerufen am 17. Juli 2008).

Maeesearch Ponemon Institute LLC, *Airport insecurity: The case of lost laptops, Executive summary*, 2008, im Internet abrufbar unter

http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf (zuletzt aufgerufen am 15. Juli 2008).

Watson, Paul, „US military secrets for sale at Afghanistan bazaar", *Los Angeles Times*, 10. April 2006.

Wooding, Steve, Anhal, Aarti und Valeri, Lorenzo, *Raising citizen awareness of information security: A practical guide*, eAware project, RAND Europe, 2003, im Internet abrufbar unter http://www.clusit.it/whitepapers/eaware_practical_guide.pdf (zuletzt aufgerufen am 17. Juli 2008).

Woody, Carol und Clinton, Larry, *Common sense guide to cyber security for small businesses — Recommended actions for information security*, Internet Security Alliance, 2004, im Internet abrufbar unter http://www.us-cert.gov/reading_room/CSG-small-business.pdf (zuletzt aufgerufen am 17. Juli 2008).

Anhänge

Anhänge – Vorlagen und Muster

Anhang I – Vorlage für die Erfassung von Zielgruppendaten

Zielgruppe			
Definition			
Kategorie		Interessen, Bedürfnisse	
Unterkategorie		Kenntnisstand	
Größe/Dimension		Kanal	
Geografischer Standort			

Beispiel/ Empfehlungen	

Anhang II – Muster für eine Ausschreibung

Der <XYZ>, ein neu gegründeter Verband mit Sitz in <Ort>, sucht ein oder mehrere Beratungsunternehmen, die ihn bei der Ausarbeitung, Durchführung und Analyse von Programmen zur Sensibilisierung für Informationssicherheit unterstützen. Einzelheiten entnehmen Sie bitte dem als Anlage beigefügten „Dienstleistungsvertrag", der mit dem/den erfolgreichen Bieter/-n abgeschlossen wird, sofern sich der Auftraggeber für ein Beratungsunternehmen entscheidet und zum Vertragsabschluss entschließt.

Ausgangssituation
Der <*XYZ*> wurde am <*Datum*> zu dem Zweck gegründet, verschiedene kommunale Behörden in <Ort> zu unterstützen und <*Aktivität*> in der Gegend zu fördern und zu koordinieren. <*Ort*> ist eine Gemeinde mit 17 500 Einwohnern. Der <*XYZ*> ist als gemeinnützige Organisation steuerbefreit; er verfügt über einen Vorstand, jedoch weder über eigene Mitarbeiter noch über eigene Räumlichkeiten. Für Beratungsleistungen stehen derzeit Haushaltsmittel in Höhe von maximal <Betrag> zur Verfügung.

Aufgabenstellung
Weiterentwicklung des Verbands und Planung der künftigen Tätigkeit mit einer Taskforce der Mitgliedsorganisationen, von der bestimmt wird, mit welchen gemeinsamen Erfordernissen sich der <*XYZ*> befassen und in welcher Weise dies geschehen soll, sowie Ausarbeitung einer Sensibilisierungskampagne. Dies umfasst im Einzelnen folgende Aufgaben:
- Konzeption eines Arbeitsplans auf der Grundlage festgelegter Ziele und Zielvorgaben
- Konzeption eines <*XYZ*>-Newsletter und Veröffentlichung der ersten Ausgaben
- Ausarbeitung der jährlichen Mittelansätze im Haushalt des <*XYZ*> für die Kampagne über die nächsten drei Jahre
- Entwicklung eines Instrumentariums zur Messung der Effektivität der Kampagne
- Ausarbeitung einer Methodik zur Erfassung der gewonnenen Erfahrungen und des Kommunikationsfeedback sowie zur Einarbeitung dieser Elemente in einen aktualisierten Arbeitsplan

Der Beginn der Kampagne ist für <*Datum*> angesetzt, die Kampagne muss bis spätestens <*Datum*> abgeschlossen sein.

Einreichung von Vorschlägen
Von interessierten Beratungsunternehmen sind bis zum <*Datum*> folgende Unterlagen an <*Kontaktperson*> beim <*XYZ*> einzureichen. Wenn Sie weitere Informationen benötigen, wenden Sie sich bitte an <*Kontaktpersonen*>.
1. Ein Vorschlag, aus dem Ihre Qualifikationen (oder die Qualifikationen des Beraterteams) hervorgehen und aus dem ersichtlich ist, wie Sie die vorstehend beschriebenen Aufgaben auszuführen beabsichtigen.
2. Eine genaue Kalkulation der anfallenden Honorare sowie eine Kalkulation der entstehenden Kosten.
3. Lebensläufe aller zur Mitwirkung an dem Projekt vorgesehenen Berater.
4. Namen und Telefonnummern von Kontaktpersonen bei mindestens drei gemeinnützigen Organisationen, für die Sie während der letzten 18 Monate tätig waren und an die wir uns wegen Referenzen wenden können.
5. Die in die engere Wahl genommenen Bieter werden in der Woche <*Datum*> zu einem persönlichen Gespräch eingeladen.

Anhang III – Vorlage für den wöchentlichen Statusbericht

WÖCHENTLICHER STATUSBERICHT

Datum

Projekt/Programm

Beteiligte und Organisation

In der vergangenen Woche erledigte Aufgaben

Für die kommende Woche anstehende Aufgaben

Risiken
Vorfälle, die möglicherweise eintreten und Pläne und Aktivitäten beeinflussen können

Beschreibung	Ursache	Möglicher Schweregrad	Wahrscheinlich-keitsgrad	Plan/Pläne zur Risikominderung

Probleme
Vorfälle, die bereits eingetreten sind und Pläne und Aktivitäten beeinflussen

Beschreibung	Ursache	Schweregrad	Status	Plan/Pläne zur Risikominderung

Planung für die kommende Woche
Wo Sie sich aufhalten und was Sie vorhaben (Urlaub/Schulung/Workshop/Arbeit für andere Auftraggeber usw.)

Tag	Vormittag	Nachmittag
Montag		
Dienstag		
Mittwoch		
Donnerstag		
Freitag		

Anhang IV – Muster für einen Arbeitsplan

Aktivitäten Führen Sie alle Aktivitäten mit einer kurzen Beschreibung sowie zugehörigen Teilaktivitäten auf (Hauptzweck usw.)	Vorgesehenes Startdatum der Aktivität	Vorgesehenes Enddatum der Aktivität	Ergebnisse Geben Sie für jede der aufgeführten Aktivitäten das erwartete Ergebnis/die erwarteten Ergebnisse an
I. Planung, Beurteilung und Konzeption			
- Vorläufiges Programmteam aufstellen	April 2006	April 2006	- Team steht
- Veränderungsmanagement-Konzept entwickeln	April 2006	April 2006	- Programmgrundsätze sind festgelegt
- Unterstützung und Mittelbereitstellung durch die Führungsebene sicherstellen	April 2006	Juni 2006	- ausdrückliche Unterstützung der Führungsebene, Budget genehmigt
- Bedarf an Personal und Sachmitteln für das Programm bestimmen	Mai 2006	Mai 2006	- Übersicht Personal und Sachmittel
- Mögliche Lösungen bewerten	Mai 2006	Juni 2006	- Entscheidung über interne Durchführung oder Fremdvergabe - nach Prioritäten geordnete Übersicht der Optionen - Programmpolitik und -verfahren - Vorlagen für Programmberichterstattung - Rollen und Verantwortungsbereiche
- Lösungsansatz auswählen und Auftrag vergeben	Juli 2006	Juli 2006	- Vertrag unterzeichnet
- Arbeitsplan ausarbeiten	Juni 2006	Juni 2006	- Arbeitsplan
- Ziele und Zielvorgaben bestimmen	Juni 2006	Juli 2006	- Ziele und Zielvorgaben des Programms formalisiert und festgelegt
- Zielgruppen bestimmen	Juni 2006	Juli 2006	- Zielgruppen bestimmt und deren Bedürfnisse dokumentiert
- Programm und Aufgabenkatalog ausarbeiten	Juni 2006	Juli 2006	- Programm ausgearbeitet
- Kommunikationsplan festlegen	Juni 2006	Juli 2006	- Botschaft festgelegt - Botschaft ausgearbeitet - Botschaft getestet - Kommunikationspartner bestimmt - Kommunikationskanäle ausgewählt - detaillierter Kommunikationsplan - Feedback-Mechanismus
- Erfolgsindikatoren für das Programm festlegen	Juni 2006	Juli 2006	- Messgrößen für die Evaluierung
- Ausgangsbasis der Evaluierung bestimmen	Juni 2006	Juli 2006	- Bewertung der Ist-Situation
- Gewonnene Erfahrungen dokumentieren	Juli 2006	Juli 2006	- gewonnene Erfahrungen erfasst

II. Ausführung und Abwicklung			
- Programmteam bestätigen	August 2006	August 2006	- Programmteam bestätigt
- Arbeitsplan überprüfen	August 2006	August 2006	- endgültiger Arbeitsplan
- Programm starten und durchführen	Oktober 2006	Januar 2007	
- Effizient kommunizieren	Oktober 2006	Januar 2007	- Kommunikationsplan umgesetzt
- Gewonnene Erfahrungen dokumentieren	Januar 2007	Januar 2007	- gewonnene Erfahrungen erfasst
III. Evaluierung und Optimierung			
- Evaluierung durchführen	Februar 2007	März 2007	- Befragungsergebnisse
- Feedback aus der Kommunikation einbeziehen	Februar 2007	März 2007	- Feedback aus Kommunikation
- Zielvorgaben des Programms überprüfen	Februar 2007	März 2007	- Zielvorgaben für das Programm
- Gewonnene Erfahrungen anwenden	März 2007	April 2007	- aktualisierte Erfahrungen
- Programm gegebenenfalls anpassen	März 2007	April 2007	- aktualisierter Arbeitsplan
- Programm wiederaufnehmen	Mai 2007		

Anhang V – Beispiel für die Zuordnung von Rollen und Themenbereichen

Rolle	**Themenbereich**											
	Vorschriften und Verfahren zur Informationssicherheit	*Sicherheit am Bildschirmarbeitsplatz*	*Strategien für den Umgang mit Websites*	*Sicherheits-bestimmungen für den E-Mail-Verkehr*	*Social Engineering*	*Sicherheits-bestimmungen für Dritte und Geschäftspartner*	*Identitätsüberprüfung*	*Technische Sicherheits-vorkehrungen*	*Einstufung und Überwachung von Informationen*	*Reaktion auf Sicherheitsvorfälle*	*Verwaltung der elektronischen Geräte (z. B. USB-Sticks, Drucker usw.)*	*usw.*
R*n*	X				X		X		X			X
R*n*+1	X			X		X				X		
R*n*+2		X				X			X	X		
R*n*+3			X	X			X		X			X
R*n*+4					X	X		X		X	X	X
R*n*+*n*	X		X	X	X	X		X	X	X		X

Anhang VI – Vorlage für ein Arbeitsblatt zur Bestandsaufnahme des Bewusstseins für Informationssicherheit

<table>
<tr><th colspan="6">ARBEITSBLATT ZUR BESTANDSAUFNAHME DES BEWUSSTSEINS
FÜR INFORMATIONSSICHERHEIT</th></tr>
<tr><td colspan="6">Name der Organisation:</td></tr>
<tr><td colspan="6">Bezeichnung des Programms:</td></tr>
<tr><td>Ziele und Zielvorgaben</td><td colspan="2">Beschreibung des Themenbereichs</td><td>Zielgruppe</td><td>Unterstützung durch die Führungs-ebene?
J/N</td><td>Ermittlung der Ausgangsbasis?
J/N</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td><td></td></tr>
<tr><td>Programmschulung erfolgt?
J/N</td><td>Datum</td><td>Nächster Schulungs-termin</td><td>Häufigkeit</td><td>Größe der Gruppe</td><td>Lokal, national, international?</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Schulungsmethoden</td><td colspan="2">Sprache</td><td colspan="3">Anmerkungen</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="3"></td></tr>
</table>

Anhang VII – Vorlage für ein Arbeitsblatt zur Ermittlung der Ausgangsbasis für eine Initiative zur Sensibilisierung für Informationssicherheit

<table>
<tr><th colspan="4">ARBEITSBLATT ZUR ERMITTLUNG DER AUSGANGSBASIS FÜR EINE INITIATIVE ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT</th></tr>
<tr><td colspan="4">Name des Überprüfers:</td></tr>
<tr><td colspan="4">Datum:</td></tr>
<tr><td colspan="4">Bezeichnung des Sensibilisierungsprogramms:</td></tr>
<tr><td colspan="4">Name des Schulungsleiters:</td></tr>
<tr><td colspan="2">Schulungsmethode:</td><td colspan="2">Sprache:</td></tr>
<tr><td colspan="2">Unterstützung durch die Führungsebene:</td><td colspan="2">Verschickte Kommunikation:</td></tr>
<tr><td colspan="4">Führen Sie die geplanten und bereits abgeschlossenen Aktivitäten in Zusammenhang mit dem Programm auf:</td></tr>
<tr><td colspan="4">Führen Sie die bereits erreichten Ziele und Zielvorgaben auf:</td></tr>
<tr><td colspan="4">Stärken:</td></tr>
<tr><td colspan="4">Schwächen:</td></tr>
<tr><td rowspan="2">Beteiligung:</td><td>Teilnehmerzahl/Gesamtzahl der bisher eingeladenen Nutzer</td><td colspan="2" rowspan="2">Gründe für Zahlenabweichungen:</td></tr>
<tr><td>Zahl der Nutzer, die angemeldet sind, aber noch nicht teilgenommen haben/ Gesamtzahl der Nutzer, die teilnehmen sollten</td></tr>
<tr><td>Bewertungs-formulare:</td><td colspan="2">Zahl der abgegebenen Bewertungsformulare/Gesamtzahl der verteilten Bewertungsformulare</td><td>Die wichtigsten abgegebenen Bemerkungen/Vorschläge:</td></tr>
</table>

Anhang VIII – Muster für einen Fragebogen zur Sensibilisierung – für Behörden

FRAGEBOGEN ZUR SENSIBILISIERUNG

[*Name der Organisation*] führt derzeit eine Studie durch, mit deren Hilfe ermittelt werden soll, wie die Einwohner von [*Ortsname*] über das Thema Informationssicherheit aufgeklärt werden können. Hätten Sie 10 Minuten Zeit, einige kurze Fragen zum Thema Informationssicherheit zu beantworten?

1. Wie gehen Sie ins Internet?
a. _____Wählverbindung
b. _____ADSL-(Breitband-)Verbindung
c. _____unternehmenseigener Internetzugang

2. Wo benutzen Sie Ihren Computer? (Zutreffendes bitte ankreuzen – Mehrfachnennungen möglich)
a. _____zu Hause
b. _____am Arbeitsplatz
c. _____öffentliche Einrichtung (Schule, Bibliothek, Gemeindezentrum)
d. _____Internet-Café
e. _____Internet-/Telefoncenter
f. _____Sonstige (bitte angeben)_____

3. Sicherheit wird häufig definiert als Schutz vor negativen Einwirkungen. Geben Sie – ausgehend von dieser Definition – auf einer Skala von 1 bis 5 an, wie besorgt Sie über die Sicherheit Ihrer elektronischen Geräte und Daten sind (Computer, Peripheriegeräte, Daten usw.) (1 = sehr besorgt, 5 = wenig besorgt):

1	2	3	4	5
Sehr		Etwas		Wenig

4. Wo sehen Sie für sich die größte Gefahr in der Informationstechnologie? (Zutreffendes bitte ankreuzen – Mehrfachnennungen möglich)
a. _____Viren und Würmer
b. _____Spam und andere unerwünschte E-Mails
c. _____Hacker
d. _____Betrugsversuche
e. _____bösartige Software (z. B. Spyware)
f. _____fehlerhafte Computerhardware
Sonstige_____

5. Ist Ihnen bekannt, dass [*Behörde*] eine Bewertung der potenziellen Risiken, die im Bereich der Informationstechnologie für die Öffentlichkeit bestehen, vornehmen will und dass Ihnen die dabei gewonnenen Informationen helfen könnten, sich vor möglichen Risiken zu schützen?
Ja, das ist mir bekannt.
Nein, das ist mir nicht bekannt.

6. Schätzen Sie auf einer Skala von 1 bis 5 Ihre Kenntnisse darüber ein, was Sie selbst unternehmen können, um Ihre Hardware und Software zu schützen (1 = sehr gute Kenntnisse, 5 = geringe Kenntnisse)

1	2	3	4	5
Sehr gut		Mittel		Gering

7. Ist Ihr Computer bzw. sind Ihre elektronischen Daten durch eine oder mehrere der folgenden Maßnahmen geschützt?

Bitte ankreuzen.
a. _____Anti-Virensoftware, die regelmäßig aktualisiert wird
b. _____Firewall
c. _____Spamfilter
d. _____guter Passwortschutz
e. _____regelmäßige Datensicherung
f. _____aktueller Internet-Browser mit Verschlüsselung
g. _____Sonstige (bitte angeben) _____

8. Auf welchem Wege möchten Sie informiert werden, wie Sie sich vor möglichen Gefahren schützen können? (Mit anderen Worten: Woher beziehen Sie in der Regel Informationen?)
a. _____Radio
b. _____TV-Spots
c. _____Tageszeitung
d. _____Newsletter, die Ihnen zugestellt werden
e. _____Bürger- und Nachbarschaftsversammlungen
f. _____Plakate
g. _____Sonstige (bitte angeben) _____

Vielen Dank für die Beantwortung unserer Fragen. Ihre Antworten helfen uns dabei, Informationen auszuarbeiten, mit denen die Öffentlichkeit dafür sensibilisiert werden kann, wie wichtig Informationssicherheit ist.

Kreuzen Sie bitte hier an, ob Sie weiter über das Thema Informationssicherheit informiert werden möchten:
o Ja
o Nein

Anhang IX – Vorlage für ein Formular zur Erfassung gewonnener Erfahrungen

<table>
<tr><td colspan="3" rowspan="2">GEWONNENE ERFAHRUNGEN</td><td>Aktenzeichen</td><td>Seite von</td></tr>
<tr><td colspan="2">Kategorie (Haupt-/Nebenkategorie):</td></tr>
<tr><td colspan="3">Bezeichnung/Thema:</td><td colspan="2">Schlüsselwörter:</td></tr>
<tr><td colspan="5">Beschreibung der Maßnahme:</td></tr>
<tr><td colspan="5">Erfahrungen:</td></tr>
<tr><td colspan="5">Empfehlungen:</td></tr>
<tr><td colspan="3">Anlagen:</td><td colspan="2">Ref.:</td></tr>
<tr><td>Vorgelegt von:</td><td>Projekt/Büro:</td><td>Org./Firma:</td><td>Ort:</td><td>Zeitpunkt des Eintretens:</td></tr>
<tr><td>Telefon:</td><td>E-Mail:</td><td>Fachgebiet:</td><td>Gebäude/Raum:</td><td>Vorlagedatum:</td></tr>
</table>

Anhang X – Muster für ein Feedback-Formular

FEEDBACK-FORMULAR

Wir freuen uns über jedes Feedback, das uns dabei hilft, unsere Sensibilisierungsinitiativen in Zukunft noch wirkungsvoller zu gestalten. Bitte geben Sie nachstehend an, wie Sie die Gesamtorganisation des Programms und die Veranstaltungsinhalte bewerten. Im Feld „Anmerkungen" haben Sie die Möglichkeit, uns Anregungen für zukünftige Initiativen zukommen zu lassen.

1 — Name und Land (Angabe freiwillig):

Gesamteindruck

2 — Wie beurteilen Sie die Qualität der Veranstaltung:

	Schlecht 1	2	3	4	Sehr gut 5
2.1 — Qualität von Veranstaltungsort und Organisation	☐	☐	☐	☐	☐
2.2 — Qualität des allgemeinen Veranstaltungsmanagements	☐	☐	☐	☐	☐
2.3 — Qualität des Programminhalts	☐	☐	☐	☐	☐
2.4 — Qualität der Veranstaltung	☐	☐	☐	☐	☐
2.5 — Gesamtbewertung der Veranstaltung	☐	☐	☐	☐	☐

Ihr persönlicher Eindruck

3 — Was würden Sie sagen:

	Schlecht 1	2	3	4	Sehr gut 5
3.1 — Der vermittelte Informationsgehalt war	☐	☐	☐	☐	☐
3.2 — Die Diskussionsrunden waren	☐	☐	☐	☐	☐
3.3 — Die Möglichkeiten zur Meinungsäußerung waren	☐	☐	☐	☐	☐
3.4 — Die Möglichkeiten zur Kenntniserweiterung waren	☐	☐	☐	☐	☐
3.5 — Der Schulungsleiter war	☐	☐	☐	☐	☐
3.6 — Das Schulungsmaterial war	☐	☐	☐	☐	☐

4 — Welches Thema/welche Themen war/waren für Sie besonders interessant?

5 — Welche Aspekte der Veranstaltung waren für Sie besonders wertvoll?

Ja Nein

6 — Würden Sie die Durchführung einer weiteren ähnlichen Initiative begrüßen?

7 — Welche Themen wären für Sie bei einer zukünftigen Veranstaltung von besonderem Interesse? Ihre Vorschläge:

Anmerkungen

8 — Platz für weitere Anmerkungen:

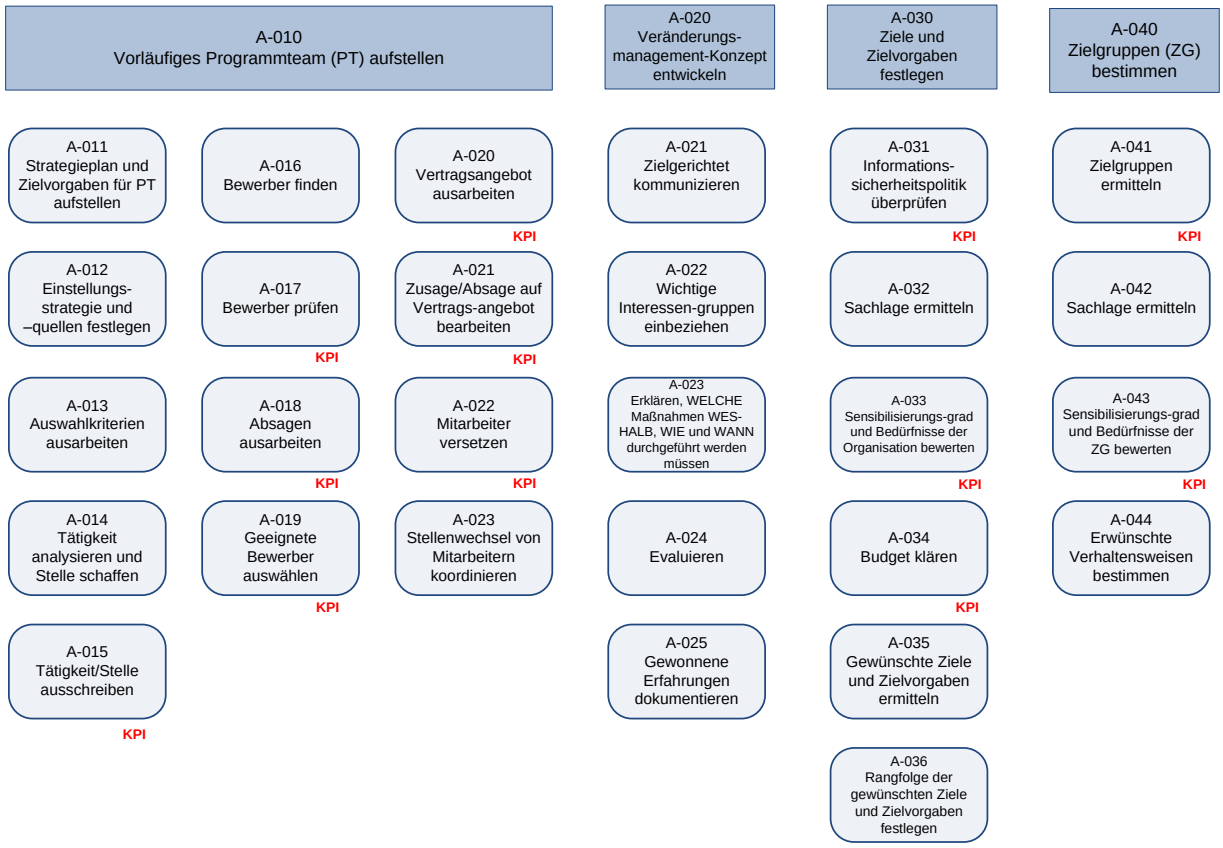
VIELEN DANK FÜR IHR FEEDBACK. GEBEN SIE DIESES BEWERTUNGSFORMULAR BITTE BEIM VERANSTALTER AB ODER LASSEN SIE ES EINFACH AN IHREM PLATZ LIEGEN, ES WIRD DANN VON UNS EINGESAMMELT.

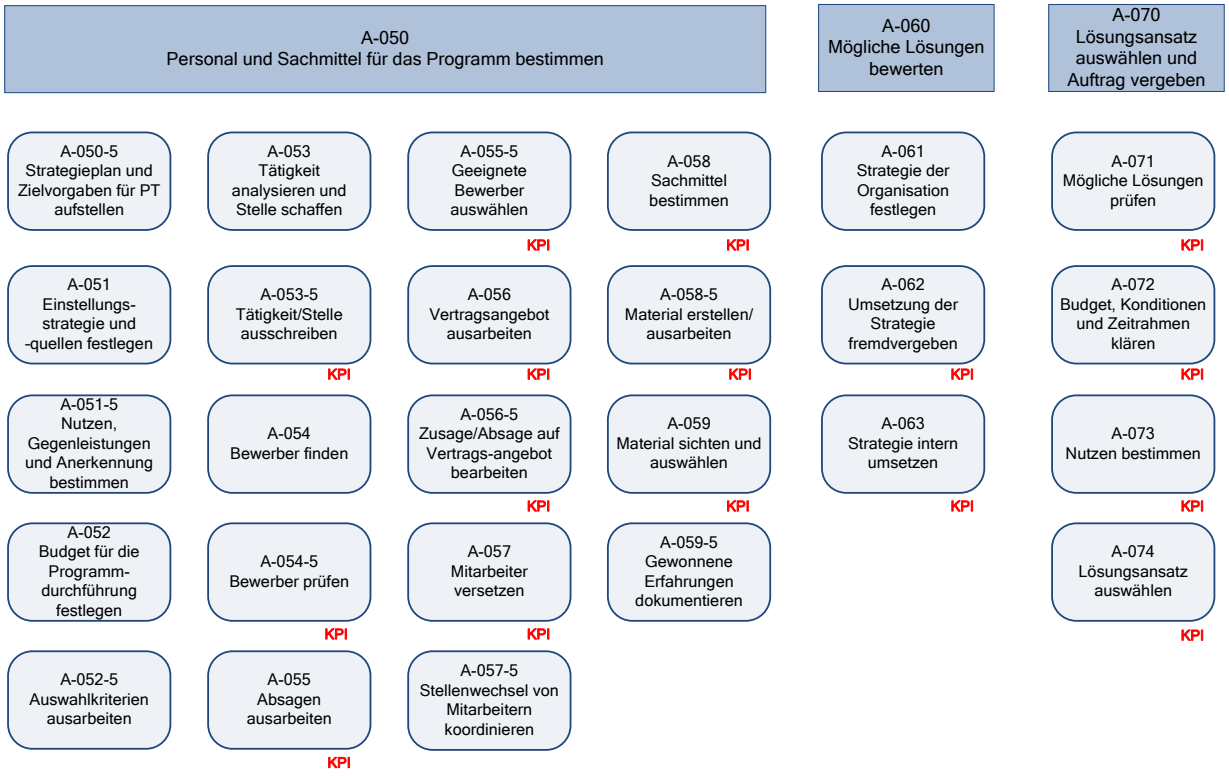
Anhang XI – Muster für ein Formular zur Meldung von Vorfällen

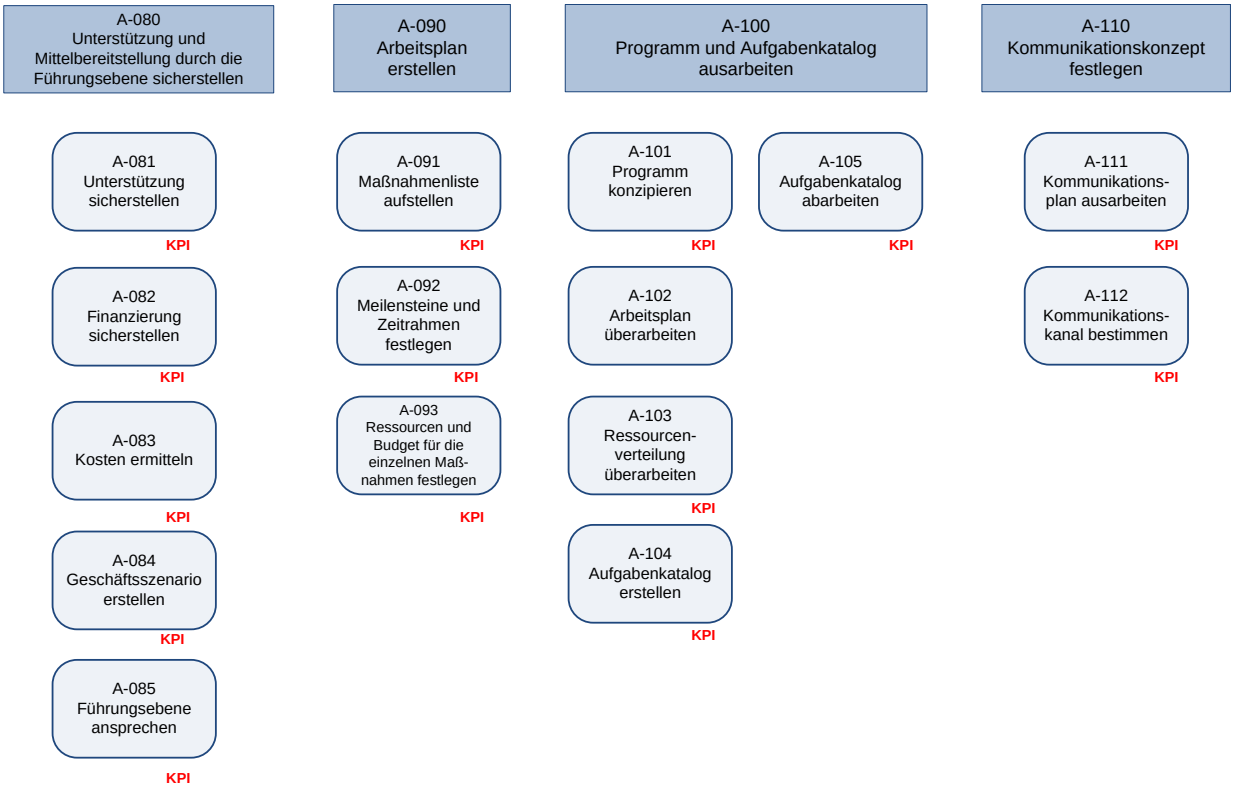
FORMULAR ZUR MELDUNG VON VORFÄLLEN	
Name:	E-Mail:
Abteilung:	Telefon:
Beschreibung des ungewöhnlichen oder verdächtigen Vorfalls:	
Datum:	
Ort:	

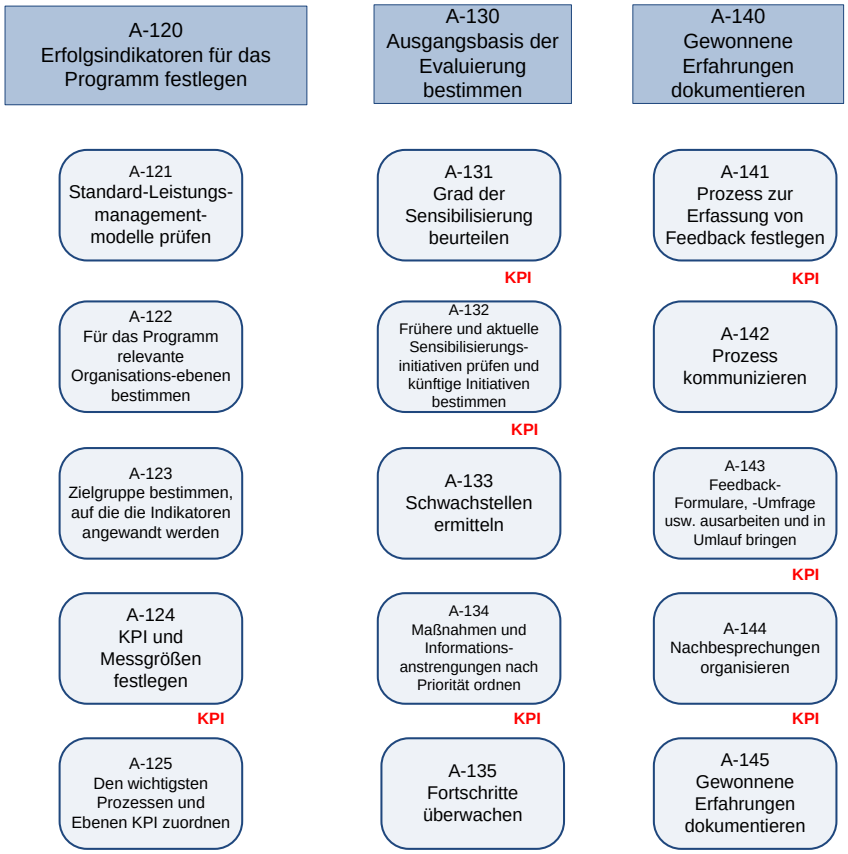
Prozesserfassung

Anhang XII – Planung, Beurteilung und Konzeption

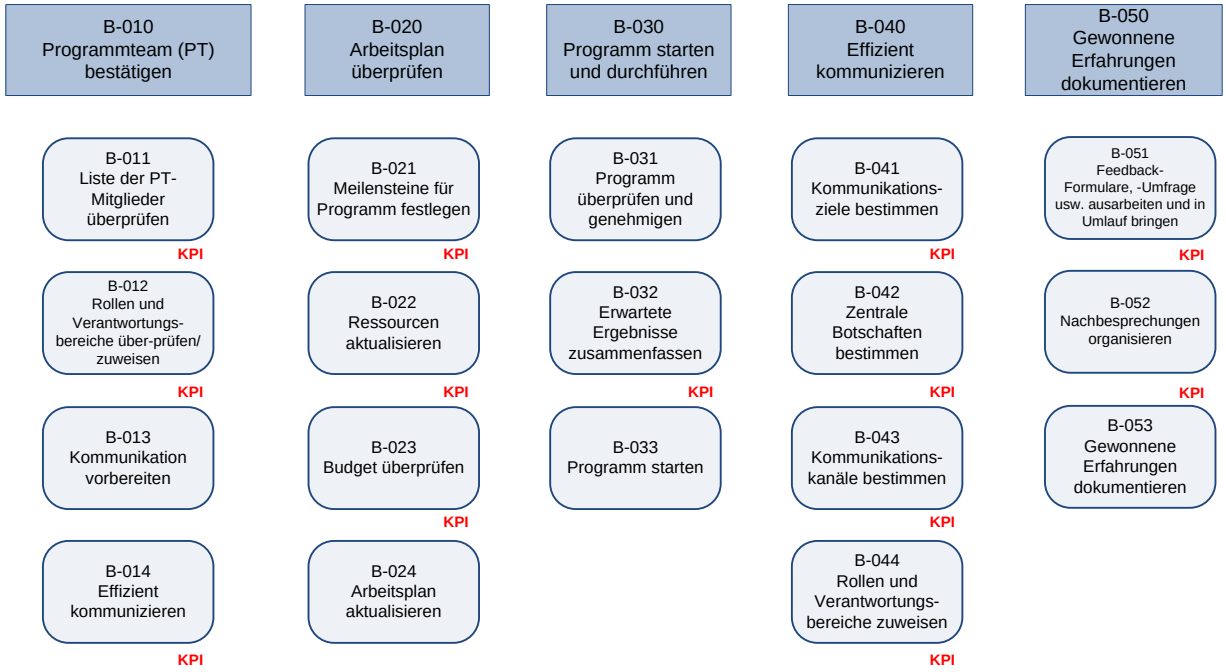



A-050
Personal und Sachmittel für das Programm bestimmen
A-060
Mögliche Lösungen bewerten
A-070
Lösungsansatz auswählen und Auftrag vergeben
A-050-5
Strategieplan und Zielvorgaben für PT aufstellen
A-051
Einstellungs-strategie und -quellen festlegen
A-051-5
Nutzen, Gegenleistungen und Anerkennung bestimmen
A-052
Budget für die Programm-durchführung festlegen
A-052-5
Auswahlkriterien ausarbeiten
A-053
Tätigkeit analysieren und Stelle schaffen
A-053-5
Tätigkeit/Stelle ausschreiben
KPI
A-054
Bewerber finden
A-054-5
Bewerber prüfen
KPI
A-055
Absagen ausarbeiten
KPI
A-055-5
Geeignete Bewerber auswählen
KPI
A-056
Vertragsangebot ausarbeiten
KPI
A-056-5
Zusage/Absage auf Vertrags-angebot bearbeiten
KPI
A-057
Mitarbeiter versetzen
KPI
A-057-5
Stellenwechsel von Mitarbeitern koordinieren
A-058
Sachmittel bestimmen
KPI
A-058-5
Material erstellen/ ausarbeiten
KPI
A-059
Material sichten und auswählen
KPI
A-059-5
Gewonnene Erfahrungen dokumentieren
A-061
Strategie der Organisation festlegen
A-062
Umsetzung der Strategie fremdvergeben
KPI
A-063
Strategie intern umsetzen
KPI
A-071
Mögliche Lösungen prüfen
KPI
A-072
Budget, Konditionen und Zeitrahmen klären
KPI
A-073
Nutzen bestimmen
KPI
A-074
Lösungsansatz auswählen
KPI

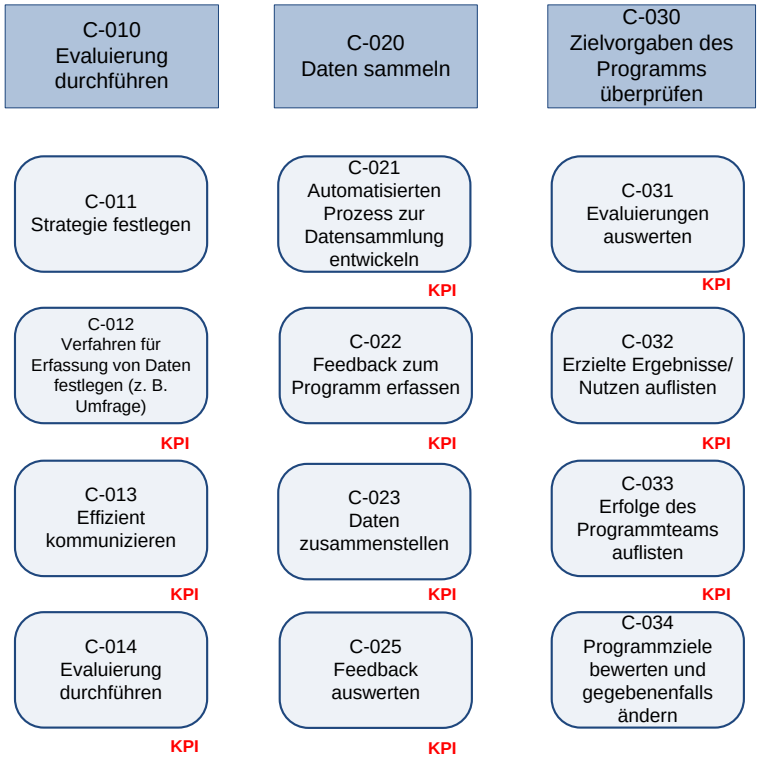

A-080
Unterstützung und Mittelbereitstellung durch die Führungsebene sicherstellen
A-081
Unterstützung sicherstellen
KPI
A-082
Finanzierung sicherstellen
KPI
A-083
Kosten ermitteln
KPI
A-084
Geschäftsszenario erstellen
KPI
A-085
Führungsebene ansprechen
KPI
A-090
Arbeitsplan erstellen
A-091
Maßnahmenliste aufstellen
KPI
A-092
Meilensteine und Zeitrahmen festlegen
KPI
A-093
Ressourcen und Budget für die einzelnen Maß-nahmen festlegen
KPI
A-100
Programm und Aufgabenkatalog ausarbeiten
A-101
Programm konzipieren
KPI
A-105
Aufgabenkatalog abarbeiten
KPI
A-102
Arbeitsplan überarbeiten
A-103
Ressourcen-verteilung überarbeiten
KPI
A-104
Aufgabenkatalog erstellen
KPI
A-110
Kommunikationskonzept festlegen
A-111
Kommunikations-plan ausarbeiten
KPI
A-112
Kommunikations-kanal bestimmen
KPI

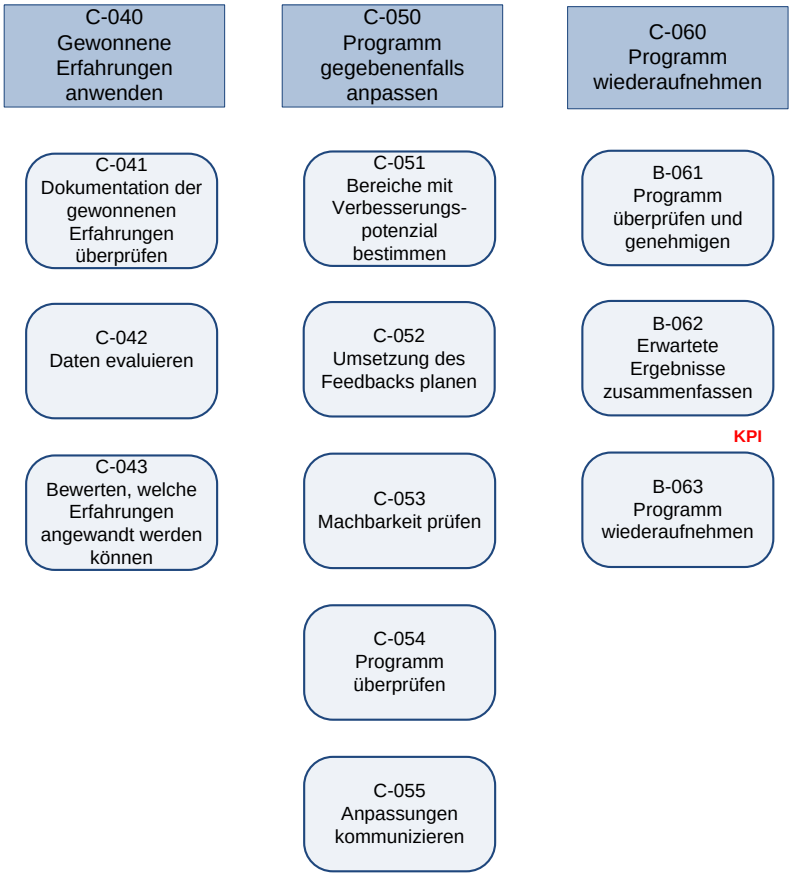

A-120
Erfolgsindikatoren für das Programm festlegen
A-121
Standard-Leistungs-management-modelle prüfen
A-122
Für das Programm relevante Organisations-ebenen bestimmen
A-123
Zielgruppe bestimmen, auf die die Indikatoren angewandt werden
A-124
KPI und Messgrößen festlegen
KPI
A-125
Den wichtigsten Prozessen und Ebenen KPI zuordnen
A-130
Ausgangsbasis der Evaluierung bestimmen
A-131
Grad der Sensibilisierung beurteilen
KPI
A-132
Frühere und aktuelle Sensibilisierungs-initiativen prüfen und künftige Initiativen bestimmen
KPI
A-133
Schwachstellen ermitteln
A-134
Maßnahmen und Informations-anstrengungen nach Priorität ordnen
KPI
A-135
Fortschritte überwachen
A-140
Gewonnene Erfahrungen dokumentieren
A-141
Prozess zur Erfassung von Feedback festlegen
KPI
A-142
Prozess kommunizieren
A-143
Feedback-Formulare, -Umfrage usw. ausarbeiten und in Umlauf bringen
KPI
A-144
Nachbesprechungen organisieren
KPI
A-145
Gewonnene Erfahrungen dokumentieren

Anhang XIII – Ausführung und Abwicklung



Anhang XIV – Evaluierung und Optimierung




C-040
Gewonnene Erfahrungen anwenden
C-041
Dokumentation der gewonnenen Erfahrungen überprüfen
C-042
Daten evaluieren
C-043
Bewerten, welche Erfahrungen angewandt werden können
C-050
Programm gegebenenfalls anpassen
C-051
Bereiche mit Verbesserungs-potenzial bestimmen
C-052
Umsetzung des Feedbacks planen
C-053
Machbarkeit prüfen
C-054
Programm überprüfen
C-055
Anpassungen kommunizieren
C-060
Programm wiederaufnehmen
B-061
Programm überprüfen und genehmigen
B-062
Erwartete Ergebnisse zusammenfassen
KPI
B-063
Programm wiederaufnehmen

Der neue Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit

ISBN: 978-92-9204-034-5

Katalognummer: TP-30-08-569-DE-C

Doi: 10.2824/14963

TP-30-08-569-DE-C

enisa
European Network and Information Security Agency

ISBN 978-92-9204-034-5

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu