# Konzept zur Durchführung von Inhouse-Schulungen zur Sensibilisierung zum Thema IT-Sicherheit

## Einleitung

Ziel der IT-Sicherheitssensibilisierung ist es, das Bewusstsein der Mitarbeiter für Sicherheitsprobleme zu schärfen. Der öffentliche Dienst als Arbeitgeber ist dazu verpflichtet, seine Angestellten zu sensibilisieren und zu belehren. Durch Schulungen zur IT-Sicherheit wird den Mitarbeitern die notwendige Kompetenz zur IT-Sicherheit vermittelt, welche sie bei der Ausführung ihrer Fachaufgaben benötigen.

Es ist sicherzustellen, dass alle Mitarbeiter die Abläufe in ihren Organisationseinheiten kennen und wissen, an wen sie sich wenden müssen, falls Sicherheitsfragen auftreten oder Sicherheitsprobleme gelöst werden müssen. Informierte und geschulte Mitarbeiter auf dem Gebiet der IT-Sicherheit sind Voraussetzungen dafür, dass alle Mitarbeiter die Folgen und Auswirkungen ihrer Tätigkeit im beruflichen und privaten Umfeld einschätzen können.

In diesem Konzept wird beschrieben, wie ein effektives Schulungs- und Sensibilisierungsprogramm zur IT-Sicherheit aufgebaut und aufrechterhalten werden kann.

## Lernziele

Die Schulungs- und Sensibilisierungsmaßnahmen verfolgen die folgenden Ziele:

- Aufmerksamkeit für IT-Sicherheit gewinnen und Interesse daran wecken
- Grundwissen zu IT-Sicherheit vermitteln
- Die für die Fachaufgaben der Mitarbeiter benötigten IT-Sicherheitskenntnisse vermitteln
- Praxiswissen vermitteln, so dass Mitarbeiter in sicherheitskritischen Situationen richtig reagieren
- Kontinuierliche Verhaltensänderungen erzielen

## Schulungsinhalte

- Einführung und Motivation
- Sensibilisierung von Benutzern
- Motivation und Aufzeigen typischer Fehler von Anwendern:
    - Leichtsinniger Umgang mit Passwörtern
    - Mangelnder Schutz von Informationen
    - Mangelndes Misstrauen
- Organisation und Sicherheit
    - Die IT-Sicherheitsvorgaben der Institution und deren Bedeutung für den Arbeitsalltag
    - Verantwortlichkeiten und Meldewege in der Institution
- Grundlagen der IT-Sicherheit
- IT-Sicherheit am Arbeitsplatz
- Bedrohungen

    - Schadsoftware (Viren, Trojaner, Würmer)
    - E-Mail und Internet
    - „Social Engineering“
- Rechtliche Aspekte (BDSG, LDSG)
- Verhalten bei Sicherheitsvorfällen
    - Erkennung und Aufbereitung von Sicherheitsvorfällen
    - Meldewege und Ansprechpartner
    - Eskalationsstrategie

## Methoden und Durchführung

Die Schulungen können in Form von Präsenzschulungen (Vortrag mit Beispielen und Übungen) in Beratungsräumen Ihrer Organisation durchgeführt werden.

Alle Inhalte werden auf die vorliegenden Bedingungen in der Organisation und die Bedürfnisse der zu schulenden Mitarbeiter abgestimmt.

## Dauer und Teilnehmerzahl

Eine Schulungsveranstaltung dauert ca. 3 Stunden und sollte eine Teilnehmeranzahl von 30 nicht überschreiten.

## Wissen regelmäßig aktualisieren

Neue IT-Anwendungen und IT-Systeme, aber auch neue Bedrohungen, Schwachstellen und mögliche Abwehrmaßnahmen machen eine ständige Auffrischung und Erweiterung des Wissens über IT-Sicherheit erforderlich. Das Schulungskonzept wird regelmäßig überprüft und ggf. angepasst. Auffrischungs- und Ergänzungskurse können für die Mitarbeiter in Absprache jederzeit angeboten werden.

## Gebühren

Für einen Schulungstag entsteht eine Gebühr von insgesamt 794,00 € zzgl. eventueller Fahrkosten des Dozenten bei Schulungen außerhalb von Potsdam. Je nach Bedarf können pro Schulungstag eine oder zwei Schulungsveranstaltungen durchgeführt werden.

## Live-Hacking

Zusätzlich oder alternativ bieten wir Ihnen an, live dabei zu sein, wenn Smartphones oder Logindaten geknackt werden – eine verblüffend direkte Form der Wissensvermittlung, der Lerneffekt ist enorm! Ab einem Preis von 1960,00 € pro Schulungstag können bis zu drei Veranstaltungen (pro Tag) durchgeführt werden.

## Kontakt

IT-Schulungszentrum des ZIT-BB, Dörte Wolf, Tel. 0331 39-2600