dsb
datenschutzbeauftragte
des kantons zürich

Anleitung

Sensibilisierung der Mitarbeitenden für Informationssicherheit

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

1 Einleitung

Die Sensibilisierung und Ausbildung der Mitarbeitenden in Bezug auf Informationssicherheit sind Voraussetzungen, um die von der Schule festgelegten Ziele im Bereich Informationssicherheit zu erreichen und langfristig halten zu können.

Dazu müssen dem Bedürfnis der Mitarbeitenden angepasste Schulungsaktivitäten geplant und kontinuierlich durchgeführt werden. Ziel ist, sicherzustellen, dass die Mitarbeitenden

- wissen, was von ihnen im Hinblick auf die Informationssicherheit erwartet wird;
- ein Bewusstsein für Informationssicherheit entwickeln und
- das notwendige Wissen im Bereich Informationssicherheit besitzen.

Diese Anleitung zeigt, wie und mit welchen Mitteln und Inhalten eine Sensibilisierung geplant, umgesetzt und aufrechterhalten werden kann.

Dieses Dokument basiert auf den Grundlagen, die das deutsche Bundesamt für Sicherheit in der Informationstechnik veröffentlicht hat, namentlich auf dem Baustein ORP.3 «Sensibilisierung und Schulung» und den dazu weiterführenden Massnahmen.

1.1 Abgrenzung

Mitarbeitende mit speziellen Rollen wie die Informationssicherheitsverantwortlichen müssen zusätzlich zu diesen Kursen fachspezifisch instruiert werden.

2 Planung eines Sensibilisierungs- und Ausbildungsprogramms

Erste Voraussetzung für die Planung und Umsetzung eines Sensibilisierungs- und Ausbildungsprogramms ist die Unterstützung durch die oberste Leitung, die bei der Gemeinde für die Informationssicherheit verantwortlich ist.

Als zweiter Schritt ist ein Programm auf der Basis der Leitlinie zur Informationssicherheit zu erarbeiten. Dieses kann Kurse, Trainingsprogramme, Sicherheitskampagnen und andere Aktivitäten zu verschiedenen Themen beinhalten.

Es sind zu definieren:

- die Person, die für das Programm verantwortlich ist
- die Ziele, die erreicht werden sollen
- die Zielgruppen
- die Themen, mit welchen diese Ziele erreicht werden können
- die Form, in welcher die Sensibilisierung zu Sicherheitsfragen stattfinden soll

2.1 Programmverantwortliche

Für die Initiierung des Sensibilisierungs- und Ausbildungsprogramms und für dessen Konzeption können sowohl die Gemeindeschreiberin / der Gemeindeschreiber, die Datenschutzberatenden als auch die Informationssicherheitsverantwortlichen zuständig sein.

Die Umsetzung erfolgt durch die für das jeweilige Thema zuständigen Rollentragenden, grösstenteils durch die Informationssicherheitsverantwortlichen. Zusätzlich können externe Schulungsanbieter in Anspruch genommen werden.

2.2 Ziele

Ziele eines solchen Sensibilisierungs- und Ausbildungsprogramms zur Informationssicherheit können sein:

- Bewusstsein für Informationssicherheit schaffen
- Grundwissen für Informationssicherheit vermitteln
- Spezifische Kenntnisse für die jeweiligen Fachaufgaben bezüglich Informationssicherheit vermitteln
- Wissen vermitteln, wie bei sicherheitskritischen Situationen zu reagieren ist
- Kontinuierliche Verhaltensänderung erzielen

2.3 Zielgruppen

Zielgruppen können sein:

- die Gemeinderäte, die Gemeindepräsidentin / der Gemeindepräsident
- Behördenmitglieder
- die Gemeindeschreiberin / der Gemeindeschreiber
- die Mitarbeitenden
- Administratorinnen / Administratoren
- allenfalls externe Mitarbeitende

Die Zielgruppen können je nach Bedarf oder Grösse der Schule einzeln oder zusammen angesprochen werden.

2.4 Module und Themen

Als Grundsatz kann festgehalten werden, dass alle Ausbildungsangebote auf die Bedürfnisse der jeweiligen Zielgruppe abgestimmt sein sollten. Dafür und um eine gewisse Flexibilität bei der Ausführung zu ermöglichen, kann ein Programm erstellt werden, das in Form von Modulen durchgeführt wird. Diese Module können je nach Relevanz den unterschiedlichen Zielgruppen zugewiesen werden.

Weitere Abstufungen sind nützlich. Bei der Einarbeitung von neuen Mitarbeitenden müssen andere Themen und Inhalte behandelt werden als bei der Vermittlung von Grundlagenwissen an alle Mitarbeitenden. Es ist von Vorteil, die Themen zusätzlich in die Anwendungsschulung zu integrieren.

Mögliche Module und Themen sind:

- Grundlagen der Informationssicherheit
- Grundprinzipien der Informationssicherheit wie Vertraulichkeit und Integrität, Sicherheits-strukturen in der Schule, Passwörter, Nutzung von E-Mail und Internet usw.
- Informationssicherheit am Arbeitsplatz
- Sicherheitsvorgaben, Sensibilisierung der Mitarbeitenden, Verhalten bei Sicherheitsvorfällen usw.
- Überblick über die rechtlichen Grundlagen
- Sicherheitsvorgaben, rechtliche Aspekte, Verhalten bei Sicherheitsvorfällen usw.
- Sicherheitsrichtlinien, -weisungen- und -konzepte der Gemeinde

2.5 Formen der Sensibilisierung und Ausbildung

Eine Auswahl möglicher Formen der Sensibilisierung und Ausbildung sind:

- Veranstaltungen (Schulungen, Videovorführungen, Besprechung von Zeitungsartikeln)
- E-Mails zu aktuellen Sicherheitsfragen
- Poster und Broschüren
- E-Learning-Programme
- Workshops
- Externe Seminare

3 Umsetzung

3.1 Modell eines Sensibilisierungs- und Ausbildungsprogramms

3.1.1 Modul «Grundlagen der Informationssicherheit»

Form	Einführungsveranstaltung
Themen	Passwörter, Anlaufstelle, Weisungen, Datenschutz (Lernprogramm Datenschutz der DSB)
Hilfsmittel	Lernprogramm der DSB, Passwortcheck der DSB
Kursleitende	Informationssicherheitsverantwortliche
Zeitraum	Stellenantritt, Antritt des öffentlichen Amtes
Lernziele	Bewusstsein schaffen, Grundwissen vermitteln

3.1.2 Modul «Richtlinien und Weisungen

Form	Publikation Intranet, Besprechung an der Teamsitzung
Themen	Neu erstellte oder veränderte Informationssicherheitsrichtlinien und -weisungen werden an einem für alle Mitarbeitenden zugänglichen Ort gespeichert und an der Teamsitzung besprochen
Kursleitende	Informationssicherheitsverantwortliche
Zeitraum	Bei Einführung oder grösseren Änderungen von Richtlinien oder Weisungen
Lernziele	Bewusstsein schaffen, Richtlinien und Weisungen kommunizieren und bekannt machen, Verhaltensänderung erzielen

3.1.3 Modul «Aktuelle Risiken»

Form	Besprechung eines Zeitungsartikels
Themen	Malware, neue/akute Gefahren
Kursleitende	Informationssicherheitsverantwortliche
Zeitraum	Aktueller Anlass
Lernziele	Bewusstsein schaffen, Verhaltensänderung erzielen

3.1.4 Modul «Datenschutztag»

Form	Videovorführung
Thema	Aktuelles Thema
Kursleitende	Informationssicherheitsverantwortliche
Zeitraum	Jährlich, beispielsweise anlässlich des Europäischen Datenschutztages (28. Januar)
Lernziele	Bewusstsein schaffen, Verhaltensänderung erzielen

3.1.5 Modul «Referat»

Form	Referat
Thema	Aktuelles Sicherheitsthema von praktischem Nutzen
Kursleitende	Informationssicherheitsverantwortliche Externe Beraterinnen und Berater
Zeitraum	Jährlich
Lernziele	Bewusstsein schaffen, Grundwissen vermitteln, angemessenes Reagieren bei sicherheitskritischen Situationen, Verhaltensänderung erzielen

3.1.6 Modul «Fachapplikationsschulung»

Form	Fachapplikationsschulung
Thema	Sicherheitsfunktionen der Software
Kursleitende	IT-Verantwortliche / Softwarelieferant
Zeitraum	Im Rahmen der Softwareschulung
Lernziele	Spezifische Fachkenntnisse vermitteln

4 Überprüfung / Verbesserung

4.1 Überprüfung und Korrekturmassnahmen

Die oder der Informationssicherheitsverantwortliche prüft regelmässig durch Stichproben, ob die Informationssicherheit integrierter Teil des Arbeitsalltags ist. Dies zeigt sich etwa darin, dass die Mitarbeitenden ihren PC in der Pause sperren oder ihre Ausdrucke nicht im Drucker liegen lassen. Vorkommnisse sind zu protokollieren und bei einer Häufung sind Korrekturmassnahmen zu treffen.

4.2 Kontinuierliche Verbesserung

In den sich dynamisch entwickelnden IT-Bereichen verliert einmal erworbenes Wissen rasch an Wert. Neue Anwendungen und IT-Systeme, aber auch neue Bedrohungen, Schwachstellen und Abwehrmassnahmen machen eine ständige Auffrischung und Erweiterung des Wissens über Informationssicherheit erforderlich. Vor diesem Hintergrund ist es wichtig, die Ausbildungskonzepte regelmässig zu aktualisieren.

5 Links

- Diverse Dokumente zum Thema Datenschutz und Informationssicherheit
- Mitarbeitergerecht aufbereitete Themenvorschläge
- Baustein ORP.3 Sensibilisierung und Schulung
- Anwendung zur Überprüfung der Sicherheit von Passwörtern
- Aktuelle Informationen über die Informationssicherheitslage in der Schweiz