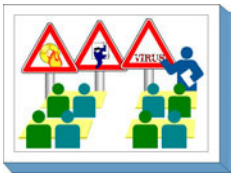
B 1.13 Sensibilisierung und Schulung zur Informationssicherheit



Beschreibung

In diesem Baustein wird beschrieben, wie ein effektives Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit aufgebaut und aufrechterhalten werden kann.

Es ist nur dann möglich, Informationssicherheit innerhalb einer Institution erfolgreich und effizient zu verwirklichen, wenn alle Mitarbeiter erkennen und akzeptieren, dass sie ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und wenn sie bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen. Hierfür müssen eine Sicherheitskultur und ein Sicherheitsbewusstsein (Awareness) aufgebaut und gepflegt werden. Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Denn je mehr sie sich damit auskennen, desto eher akzeptieren sie entsprechende Sicherheitsmaßnahmen. Sie müssen auch über die erforderlichen Kenntnisse verfügen, um Maßnahmen richtig verstehen und anwenden zu können. Insbesondere muss ihnen bekannt sein, was von ihnen im Hinblick auf Informationssicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten.

Um den Mitarbeitern das nötige Wissen zu vermitteln, sind gleichermaßen Sensibilisierungs- und Schulungsmaßnahmen erforderlich. Ziel der Sensibilisierung für Informationssicherheit ist es, die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen. Durch Schulungen zur Informationssicherheit sollen die Mitarbeiter die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten erwerben.

Eine angemessene Informationssicherheit sollte von allen Mitarbeitern als selbstverständlicher Teil ihrer Arbeitsumgebung verinnerlicht werden. Dies setzt in vielen Bereichen eine langfristige Verhaltensänderung voraus, besonders wenn Informationssicherheit mit Komfort- oder Funktionseinbußen verbunden ist. Um hier nachhaltige Ergebnisse zu erzielen, ist ein kontinuierlicher Prozess erforderlich. Daher muss die Institution ein durchgängiges Sensibilisierungs- und Schulungsprogramm zur Informationssicherheit erarbeiten und etablieren. Es sollte bereits bei der Einstellung von Mitarbeitern beginnen, unterschiedliche Zielgruppen mit deren Fähigkeiten, Arbeitsabläufen und benötigten Ressourcen berücksichtigen und die Mitarbeiter auch begleiten, wenn sich ihre Aufgaben oder Positionen verändern.

Gefährdungslage

Für den IT-Grundschutz werden in diesem Baustein die folgenden typische Gefährdungen betrachtet:

Organisatorische Mängel

- G 2.2 *Unzureichende Kenntnis über Regelungen*
- G 2.7 *Unerlaubte Ausübung von Rechten*
- G 2.102 *Unzureichende Sensibilisierung für Informationssicherheit*
- G 2.103 *Unzureichende Schulung der Mitarbeiter*
- G 2.105 *Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen*
- G 2.141 *Nicht erkannte Sicherheitsvorfälle*
- G 2.201 *Unzureichende Berücksichtigung von Veränderungen im Arbeitsumfeld von Mitarbeitern*

Menschliche Fehlhandlungen

- G 3.1 *Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten*
- G 3.3 *Nichtbeachtung von Sicherheitsmaßnahmen*
- G 3.6 *Gefährdung durch Reinigungs- oder Fremdpersonal*
- G 3.8 *Fehlerhafte Nutzung von IT-Systemen*
- G 3.9 *Fehlerhafte Administration von IT-Systemen*
- G 3.44 *Sorglosigkeit im Umgang mit Informationen*
- G 3.77 *Mangelhafte Akzeptanz von Informationssicherheit*

Vorsätzliche Handlungen

- G 5.1 *Manipulation oder Zerstörung von Geräten oder Zubehör*
- G 5.2 *Manipulation an Informationen oder Software*
- G 5.9 *Unberechtigte IT-Nutzung*
- G 5.19 *Missbrauch von Benutzerrechten*
- G 5.20 *Missbrauch von Administratorrechten*
- G 5.42 *Social Engineering*
- G 5.102 *Sabotage*
- G 5.104 *Ausspähen von Informationen*

Maßnahmenempfehlungen

Um den betrachteten Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Sensibilisierungs- und Schulungsprogramm sollte auf die Institution zugeschnitten sein und die dort vorhandene Kultur (siehe M 3.83 *Analyse sicherheitsrelevanter personeller Faktoren*) sowie das notwendige Sicherheitsniveau berücksichtigen. In diesem Rahmen sind möglichst unterschiedliche und aufeinander abgestimmte Methoden und Medien zu verwenden.

Planung und Konzeption

Es ist für den Sicherheitsprozess sehr wichtig, dass dieser aktiv vom Management unterstützt wird. Hierfür muss es den Wert von Informationssicherheit für die Ziele der Institution erkannt und verinnerlicht haben (siehe M 3.44 *Sensibilisierung des Managements für Informationssicherheit*). Wie das Management den gesamten Lebenszyklus eines Sensibilisierungs- und Schulungsprogramms wirkungsvoll unterstützen kann, beschreibt Maßnahme M 3.96 *Unterstützung des Managements für Sensibilisierung und Schulung*.

Diese Unterstützung kann z. B. mit dem expliziten Auftrag zur Konzeption entsprechender Programme beginnen. Die notwendigen Schritte sind in den Maßnahmen M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit* und M 2.557 *Konzeption eines Schulungsprogramms zur Informationssicherheit* beschrieben. Wichtig ist hier insbesondere, die Zielgruppen zu definieren (siehe M 3.93 *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*).

Beschaffung

Um Sensibilisierungs- und Schulungsmaßnahmen vorzubereiten und durchzuführen, wird internes oder externes Personal benötigt (siehe M 3.48 *Auswahl von Trainern oder externen Schulungsanbietern*).

Umsetzung

In der Umsetzungsphase werden die Mitarbeiter den vorher definierten Zielgruppen zugeordnet und zielgruppenspezifisch geeignete Inhalte für Sensibilisierungs- und Schulungsmaßnahmen ausgewählt (siehe M 3.45 *Planung von Schulungsinhalten zur Informationssicherheit*). Auch sind Maßnahmen umzusetzen, durch die bei den Mitarbeitern die Ansprechpartner für Sicherheitsfragen bekannter werden (siehe M 3.46 *Ansprechpartner zu Sicherheitsfragen*).

Darüber hinaus werden für Sensibilisierungs- und Schulungsmaßnahmen diverse Ressourcen benötigt, beispielsweise Personal, geeignete Räumlichkeiten oder spezielles Equipment. Besondere Sicherheitsaspekte, die bei der Gestaltung von Schulungsräumen zu beachten sind, finden sich in Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume*.

Betrieb, kontinuierliche Pflege und Weiterentwicklung

Für eine erfolgreiche Lernstoffvermittlung müssen die richtigen Methoden und Medien eingesetzt werden (siehe M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit* und M 3.47 *Durchführung von Planspielen zur Informationssicherheit*).

Ein weiterer wichtiger Bestandteil von Schulungen zur Informationssicherheit ist der Umgang mit der Informationstechnik (siehe M 3.26 *Einweisung des Personals in den sicheren Umgang mit IT* und wei-

tere themenspezifische Maßnahmen). Besonders wenn neue Techniken eingeführt werden, sollten die Mitarbeiter frühzeitig über diese informiert sowie für Gefahrenpotenziale und Sicherheitsmaßnahmen sensibilisiert werden.

Um die Präsenz von vermittelten Lerninhalten zu verbessern, können Methoden der Lernstoffsicherung eingesetzt werden (siehe M 3.95 *Lernstoffsicherung*). Auch sollte regelmäßig überprüft werden, ob die Sensibilisierungs- und Schulungsmaßnahmen erfolgreich sind (siehe M 3.94 *Messung und Auswertung des Lernerfolgs*). Bei Bedarf müssen sie angepasst werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Sensibilisierung und Schulung zur Informationssicherheit" vorgestellt.

Planung und Konzeption

- M 2.312 (A) *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit*
- M 2.557 (A) *Konzeption eines Schulungsprogramms zur Informationssicherheit*
- M 3.44 (A) *Sensibilisierung des Managements für Informationssicherheit*
- M 3.51 (Z) *Geeignetes Konzept für Personaleinsatz und -qualifizierung*
- M 3.83 (Z) *Analyse sicherheitsrelevanter personeller Faktoren*
- M 3.93 (A) *Analyse der Zielgruppen für Sensibilisierungs und Schulungsprogramme*
- M 3.96 (A) *Unterstützung des Managements für Sensibilisierung und Schulung*

Beschaffung

- M 3.48 (Z) *Auswahl von Trainern oder externen Schulungsanbietern*

Umsetzung

- M 3.45 (A) *Planung von Schulungsinhalten zur Informationssicherheit*
- M 3.46 (A) *Ansprechpartner zu Sicherheitsfragen*
- M 3.49 (B) *Schulung zur Vorgehensweise nach IT-Grundschutz*

Betrieb

- M 2.198 (A) *Sensibilisierung der Mitarbeiter für Informationssicherheit*
- M 3.26 (A) *Einweisung des Personals in den sicheren Umgang mit IT*
- M 3.47 (Z) *Durchführung von Planspielen zur Informationssicherheit*
- M 3.94 (C) *Messung und Auswertung des Lernerfolgs*
- M 3.95 (Z) *Lernstoffsicherung*