



Umsetzungshinweise zum Baustein INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

- Einleitung
- Maßnahmen
 - Maßnahmen zum Baustein INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- Weiterführende Informationen
 - Wissenswertes
 - Quellenverweise

1. Einleitung

In der Regel hat jede Institution einen oder mehrere Räume, in denen Besprechungen, Schulungen oder sonstige Veranstaltungen durchgeführt werden können. Hierfür sind oft speziell ausgestattete Räume vorgesehen. Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im Wesentlichen dadurch aus, dass sie von wechselnden Personen bzw. Personenkreisen, Personal und Besuchern genutzt werden. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie beispielsweise fremde Laptops an fest verbauten Beamern. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume*

INF.10.M1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen (B)

Für die Nutzung dieser Räume und der darin vorhandenen Technik sollte es in jeder Institution feste Regeln geben. Diese sollten unter anderem Verhaltenshinweisen genereller Art für die Benutzer umfassen, aber auch solche, um fest installierte sowie mitgebrachte Geräte, Datenträger und Arbeitsmaterialien benutzen zu können. Es muss geklärt werden, unter welchen Rahmenbedingungen Externe mitgebrachte IT-Systeme, wie Mobiltelefone und Laptops, einsetzen dürfen. Vorhandene Festnetz-Telefonanschlüsse müssen vor Missbrauch geschützt werden, beispielsweise indem externe Nummern nur angewählt werden können, nachdem ein geeignetes Passwort eingegeben wurde. Im Raum sollten die Telefonnummern von Ansprechpartnern für Probleme, wie IT-Support oder zur Schlüsselverwaltung, ausgehängt oder ausgelegt sein. Die Ansprechpartner müssen jederzeit während der üblichen Bürozeiten erreichbar sein. Wenn im Raum Beamer und weitere Geräte fest eingerichtet sind, müssen erforderliche Sicherheitsmaßnahmen zum Schutz dieser Geräte vor Diebstahl getroffen werden. Beispielsweise können diese mit Diebstahlsicherungen wie Stahlkabel versehen werden. Auch verschließbare Schränke für Materialien sind sinnvoll. Nach Ende jeder Veranstaltung sollten die Materialien entfernt werden, die vertrauliche Informationen enthalten könnten. Daher sollten z. B. benutztes Flipchart-Papier mitgenommen und die Tafeln gesäubert werden. Auch im Papierkorb entsorgte vertrauliche Entwürfe dürfen nicht vergessen werden. Beim Verlassen sollten Materialien in Schränken und der Raum an sich verschlossen werden. Verlassen die Mitarbeiter, die die Besucher beaufsichtigen, den Raum, muss der Besuch von einem anderen internen Mitarbeiter beaufsichtigt werden.

Zudem ist festzulegen, wer für die Administration der vorhandenen Schulungs- und Präsentationsrechner zuständig ist. Außerdem sollten Hinweise auf Fluchtwege und das richtige Verhalten bei Bränden nicht vergessen werden (siehe INF.1. *Allgemeines Gebäude*).

INF.10.M2 ENTFALLEN (B)

Die zugehörige Anforderung im Baustein ist entfallen.

INF.10.M3 Geschlossene Fenster und Türen (B)

Fenster und nach außen gehende Türen (Balkone, Terrassen) müssen in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. Außentüren sollten generell abgeschlossen werden. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen, bieten offene Fenster und Türen Einbrechern ideale Einstiegsmöglichkeiten, die auch während der Betriebszeiten einer Institution missbraucht werden können.

Mitarbeiter sollten darauf hingewiesen werden, dass generell Fenster und in Räumlichkeiten, in denen sich IT-Systeme und sensitive Dokumente befinden, zusätzlich die Türen beim Verlassen abgeschlossen werden müssen.

Brand- und Rauchschutztüren bieten nur im verschlossenen Zustand Schutz und dürfen deshalb keinesfalls durch Keile oder andere Vorrichtungen dauerhaft offen gehalten werden.

Pförtner oder Mitarbeiter der Haustechnik sollten regelmäßig überprüfen, ob die genannten Regeln eingehalten werden. Es wird empfohlen, die Schlüssel für die Besprechungs-, Veranstaltungs- und Schulungsräume von einer zentralen Stelle zu verwalten (z. B. Pforte oder innerer Dienst).

INF.10.M4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen (S)

Von der geplanten Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen hängt nicht nur die Wahl der Ausstattung ab, sondern auch die erforderlichen Sicherheitsmaßnahmen. Daher sollte zunächst dokumentiert werden, welche Nutzungsarten für welche Räume vorgesehen sind, um basierend auf den Anforderungen aus den geplanten Einsatzszenarien die Einrichtung auszuwählen und organisatorische und technische Nutzungsregelungen festzulegen.

Die Lage von Besprechungs-, Veranstaltungs- und Schulungsräumen sollte möglichst so gewählt werden, dass Fremde nicht unnötig das Haus durchqueren müssen. Der Weg zu einem Besprechungs-, Veranstaltungs- und Schulungsraum sollte möglichst nicht in die Nähe von oder gar durch besonders sicherheitsrelevante Bereiche führen. Ebenso sollten Besprechungs-, Veranstaltungs- und Schulungsräume so ausgewählt und eingerichtet sein, dass sie zu möglichst geringen Störungen des normalen Betriebs führen.

INF.10.M5 Fliegende Verkabelung (S)

In Besprechungs-, Veranstaltungs- und Schulungsräumen sollten die Stromanschlüsse so verteilt sein, dass sie sich dort befinden, wo auch die IT-Systeme angeschlossen werden können, ohne dass Kabel über Boden oder Tische verlegt werden müssen. Sollten dennoch Kabel über Laufwege verlegt werden, sollten diese mit Kabelschächten, Teppichen oder Klebeband abgedeckt bzw. fixiert werden.

INF.10.M6 Einrichtung sicherer Netzzugänge (S)

In Besprechungs-, Veranstaltungs- und Schulungsräumen sind einerseits häufig IT-Systeme wie Beamer, Schulungs- oder Präsentationsrechner fest installiert, andererseits werden dorthin auch mobile IT-Systeme wie Laptops mitgebracht. Dabei ist oft auch gewünscht, dass diese IT-Systeme miteinander, mit dem Internet oder dem institutionsinternen Intranet vernetzt werden können.

Da fremde IT-Systeme aber immer als nicht vertrauenswürdig betrachtet werden sollten, sollte eine Anbindung von durch Besucher mitgebrachten IT-Systemen an interne LANs unterbunden werden. Das Datennetz für Besucher sollten von dem der Institution getrennt werden.

Es sollte sichergestellt werden, dass Dritte den Datenverkehr bei der LAN-Nutzung durch Mitarbeiter nicht mitlesen bzw. mitschneiden können.

Es sollte darauf verzichtet werden, fremden Mitarbeitern einen Zugang zum Internet anzubieten, der das institutionsinterne Netz als Vermittlungsnetz nutzt. Es kann z. B. aufgrund von Konfigurationsfehlern nie ausgeschlossen werden, dass fremde Mitarbeiter trotz eingeschränkter Zugriffsmöglichkeiten auf schutzwürdige Informationen oder Anwendungen zugreifen können.

Die Stromversorgung in Besprechungs-, Veranstaltungs- und Schulungsräumen sollte aus der Unterverteilung heraus getrennt von den anderen Räumen der Institution aufgebaut werden. Es wird empfohlen, jeweils Überspannungsschütze in der Elektro-Unterverteilung zu verbauen und die Stromkreise zu separieren.

INF.10.M7 Sichere Konfiguration von Schulungs- und Präsentationsrechnern (S)

Um Sicherheitsprobleme und die unerwünschte Nutzung von dedizierten Schulungs- und Präsentationsrechnern zu vermeiden, sollten die IT-Systeme sicher konfiguriert werden. Dazu gehört:

- Grundinstallation: Nur die notwendigen Pakete sollten eingespielt werden,
- Löschen nicht benötigter Programme (wie beispielsweise Spiele)

Wird eine Standardkonfiguration für die Schulungsrechner festgelegt, kann der Installationsaufwand minimiert und ein Mindestniveau an Sicherheit für die IT-Systeme gewährleistet werden. Vor dem Einsatz von Schulungs- und Präsentationsrechnern sollte festgelegt werden, welche Anwendungen und Kommunikationsschnittstellen in der jeweiligen Schulung genutzt werden sollen. Vor jeder Schulung muss überprüft werden, ob die IT-Systeme für die Zwecke der Schulung geeignet konfiguriert sind. Um hier auf langwierige Prüfungen verzichten zu können, ist es sinnvoll, Schulungsrechner vor jedem Einsatz über entsprechend vorbereitete Pakete zurückzusetzen (siehe INF.10.M9 *Zurücksetzen von Schulungs- und Präsentationsrechnern*).

Von Schulungsrechnern sollten Informationen, wie Schulungs- oder Prüfungsunterlagen, nicht unkontrolliert kopiert werden können. Zudem sollte es auch nicht möglich sein, zusätzliche Dateien oder Programme aufzuspielen. Daher sollten einerseits Zugriffsrechte für die Benutzer dieser Rechner restriktiv vergeben und andererseits das Überspielen von Daten auf externe Medien verhindert werden.

INF.10.M8 Erstellung eines Nutzungsnachweises für Räume (S)

Für die Räume, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen stattfinden, sollte ein Nutzungsnachweis erstellt werden. Aus diesem Nachweis sollte hervorgehen, wer die Räume zu welchem Zeitpunkt genutzt hat. Dabei kann ein Raumbuchungssystem hilfreich sein. Mithilfe dieses Raumbuchungssystems kann dann auch eine Überschneidung vermieden werden. Es sollte nachträglich ersichtlich sein, wer die Räume genutzt hat. Ein Nutzungsnachweis kann auch für normale Besprechungsräume von Vorteil sein.

INF.10.M9 Zurücksetzen von Schulungs- und Präsentationsrechnern (H)

Bei IT-Systemen, die von wechselnden Personen genutzt werden, kann es häufiger zu Problemen mit dem Betriebssystem oder den Anwendungen kommen, die nur durch den IT-Betrieb wieder behoben werden können. Dies kann z. B. durch Softwarefehler, Konfigurationsänderungen, Aufspielen neuer Software oder Computer-Viren verursacht werden.

Damit die Administratoren bei den oben beschriebenen Problemen auf Schulungs- und Präsentationsrechnern nicht zeitaufwendig nach Fehlern suchen müssen, sollte eine Software-Reinstallation der Standardkonfiguration vorgenommen werden. Dabei ist es hilfreich, wenn sich die Systeme weitestgehend gleichen, zumindest in Bereichen mit ähnlicher Aufgabenstellung.

Eine Software-Reinstallation kann auf verschiedene Weise durchgeführt werden, so gibt es z. B. spezielle Programme, die eine vorgegebene Konfiguration von einem Server auf den neu zu installierenden Arbeitsplatzrechner überspielen. Hierbei ist zu beachten, dass solche Arbeiten meist in zweierlei Hinsicht zeitkritisch sind: Die Neueinrichtung sollte möglichst schnell erfolgen können, damit das IT-System wieder verfügbar ist und das Netz sollte möglichst wenig belastet werden. Dies ist insbesondere bei Schulungsrechnern oder PC-Pools wichtig.

Eine weitere Möglichkeit besteht darin, spezielle Hard- oder Software einzusetzen, die das IT-System nach einem Neustart auf einen definierten Ausgangszustand zurücksetzt und alle durch Benutzer vorgenommenen Änderungen damit verwirft.

INF.10.M10 Mitführverbot von Mobiltelefonen (H)

Wenn ausgeschlossen werden soll, dass vertrauliche Besprechungen und Gespräche mit Mobiltelefonen abgehört oder aufgenommen werden, sollten diese nicht in den Gesprächen mitgeführt werden. Es reicht als Schutz nicht immer aus, die Mobiltelefone in den Standby- oder Flugmodus zu bringen bzw. auszuschalten. Wenn sie entsprechend manipuliert sind, könnten sie über Funk unbemerkt eingeschaltet werden. Es kann mit einem geeigneten Detektor überprüft werden, ob das Mitführungsverbot eingehalten wird.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

[DIN1627] DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung: September 2011