Bundesamt
für Sicherheit in der
Informationstechnik

INF: Infrastruktur

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

1 Beschreibung

1.1 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. Dauerhaft werden sie vom gleichen Personenkreis meist nur kurze Zeit genutzt. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie fremde Laptops an fest verbauten Beamern. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist.

1.2 Lebenszyklus

Planung und Konzeption

Die Nutzungsmöglichkeiten von Besprechungs-, Veranstaltungs- und Schulungsräumen variieren sehr stark. Da hiervon auch die erforderlichen Sicherheitsmaßnahmen abhängen, sollte zunächst eine Nutzungsübersicht erstellt werden, in der die geplanten Einsatzszenarien berücksichtigt werden (siehe INF.10.M1 *Sichere Nutzung von Besprechungs, Veranstaltungs- und Schulungsräumen*).

Basierend auf dem Nutzungskonzept sollten geeignete Räumlichkeiten ausgewählt und ausgestattet werden (siehe INF.10.M4 *Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen)*.

Wenn auf das LAN oder das Internet zugegriffen werden soll, müssen die entsprechenden Zugänge zu den Datennetzen in Besprechungs-, Veranstaltungs- und Schulungsräumen sorgfältig abgesichert werden (siehe INF.10.*Einrichtung sicherer Netzzugänge*).

Umsetzung

Es müssen Regeln für die Sicherheit in Besprechungs-, Veranstaltungs- und Schulungsräume festgelegt sowie technisch und organisatorisch umgesetzt werden. Alle Mitarbeiter müssen darüber informiert

werden, welche Regeln für die Nutzung zu beachten sind (siehe INF.10.M1 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen* und *INF.10.M8 Erstellung eines Nutzungsnachweises für Räume*).

Betrieb

Auch in Besprechungs-, Veranstaltungs- und Schulungsräumen muss mit den Einrichtungen und der vorhandenen Technik sorgfältig umgegangen werden. Dazu gehören die Einhaltung der von der Institution vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien (siehe INF.10.M1 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen).*

Aussonderung

Gerade in Besprechungs-, Veranstaltungs- und Schulungsräumen mit häufig wechselnden Benutzern ist es wichtig, Arbeitsmaterialien wie Datenträger und Papiere sorgsam zu entsorgen und nicht einfach liegen zu lassen (siehe INF.10.M1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen).

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise im Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume" aufgeführt

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen sollten vorrangig umgesetzt werden:

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

Für die Nutzung dieser Räume und die darin vorhandene Technik sollte es in jeder Institution feste Regeln geben. Diese sollten unter anderem Verhaltenshinweise genereller Art für die Benutzer umfassen, aber auch solche, um fest installierte sowie mitgebrachter Geräte, Datenträgern 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 sollte z. B. benutztes Flipchart-Papier mitgenommen und die Tafeln gesäubert werden. Auch im Papierkorb entsorgte vertrauliche Entwürfe dürfen nicht vergessen werden. Werden die Räume verlassen, sollten Materialien in Schränken verschlossen 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 Beaufsichtigung von Besuchern (B)

Personen, die nicht der Institution angehören sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein. Wird es erforderlich, einen Externen allein in Besprechungs-, Veranstaltungs- und Schulungsräumen zurückzulassen, sollte der Besucher in der Zeit von einem anderen internen Mitarbeiter beaufsichtigt werden.

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.

Es ist sinnvoll, dass Pförtner oder Mitarbeiter der Haustechnik 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).

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich Besprechungs-, Veranstaltungs- und Schulungsraum.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume".

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, sondern auch die erforderlichen Sicherheitsmaßnahmen ab. 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 das 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 muss 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 sicherheitskritisch konfiguriert werden. Dazu gehört:

- Grundinstallation: Nur die notwendigen Pakete sollten eingespielt werden,
- Löschen nicht benötigter Programme: wie beispielsweise Spiele,
- Virenscanner: Es sollten geeignete Produkte installiert werden.

Vor dem Einsatz von Schulungs- und Präsentationsrechnern sollte festgelegt werden, welche Anwendungen und Kommunikationsschnittstellen in der jeweiligen Schulung genutzt werden sollen. Wird vorher eine Standardkonfiguration für die Schulungsrechner festgelegt, kann der Installationsaufwand minimiert und ein Mindestniveau an Sicherheit für die IT-Systeme gewährleistet werden. 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.

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

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 Leiter der IT 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 Arbeitsplatzrechnern 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 Literaturverzeichnis

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen im Bereich "Umsetzungshinweise zum Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume*" finden sich unter anderem in folgenden Veröffentlichungen:

[27001]	ISO/IEC 27001:2013: Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013
[DIN1627]	DIN EN 1627:2011-09 Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchshemmung - Anforderung und Klassifizierung: September 2011