



## INF: Infrastruktur

# 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 und Besuchern in der Regel nur für einen begrenzten Zeitraum genutzt werden. Mitgebrachte IT-Systeme werden dabei häufig gemeinsam mit Geräten der Institution betrieben, wie beispielsweise institutionsfremde Laptops an fest verbauten Beamern. Aus diesen unterschiedlichen Nutzungsszenarien heraus ergibt sich eine besondere Gefährdungslage, die in anderen Räumen der Institution in dieser Weise nicht existiert.

### 1.2 Zielsetzung

Ziel des Bausteins ist der Schutz von Informationen, die in Besprechungs-, Veranstaltungs- und Schulungsräumen bearbeitet werden, sowie der IT-Systeme, die in diesen Räumen betrieben werden. Außerdem wird der empfohlene Umgang mit Besuchern, die die entsprechenden Räume nutzen, behandelt.

### 1.3 Abgrenzung und Modellierung

Der Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* ist für alle Räume anzuwenden, die für Besprechungen, Veranstaltungen oder Schulungen genutzt werden.

Dieser Baustein betrachtet alle technischen und nicht-technischen Sicherheitsaspekte zur Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen. Detaillierte Empfehlungen, wie die IT-Systeme in diesen Räumen konfiguriert und abgesichert werden können, werden nicht in diesem Baustein behandelt. Sie sind in SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen System-Bausteinen zu finden. Weitere für Besprechungsräume relevante Sicherheitsaspekte, wie z. B. für WLANs oder Videokonferenzenanlagen, werden in den Bausteinen der Schichten NET.2 *Funknetze* bzw. NET.4 *Telekommunikation* betrachtet. Die Verkabelung in diesen Räumen wird im Baustein INF.12 *Verkabelung* gesondert berücksichtigt. Anforderungen zum Brandschutz sind im Baustein INF.1 *Allgemeines Gebäude* zu finden. Anforderungen zur Beaufsichtigung von Besuchern sind im Baustein

ORP.1 *Organisation* zu finden.

## 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* von besonderer Bedeutung:

### 2.1 Fehlende oder unzureichende Regelungen

Wenn z. B. Mitarbeiter die Fenster und Türen nach Verlassen eines Besprechungs-, Veranstaltungs- oder Schulungsraumes nicht schließen oder vertrauliche Informationen von einem Whiteboard oder Flipchart nicht entfernt werden, können diese Informationen unberechtigt eingesehen werden. Generell sollten den Mitarbeitern daher entsprechende Regelungen an die Hand gegeben werden, sodass entsprechende Sicherheitslücken nicht auftreten können. Regelungen lediglich festzulegen sichert aber noch nicht, dass sie auch beachtet werden und der Betrieb störungsfrei ist. Viele Probleme entstehen, wenn Regelungen zwar vorhanden, aber den Mitarbeitern nicht bekannt sind. Oft wissen Mitarbeiter z. B. nicht, dass Fenster und Türen nach Besprechungen verschlossen werden müssen oder wie sie mit einem genutzten Flipchart umgehen sollen.

### 2.2 Inkompatibilität zwischen fremder und eigener IT

IT-Systeme werden immer mobiler und zunehmend in unterschiedlichen Umgebungen verwendet. Oft finden Benutzer Szenarien vor, in denen die eigenen IT-Systeme nicht wie geplant genutzt werden können, da sie nicht mit den fremden IT-Systemen kompatibel sind. Beispielsweise verfügen ältere Geräte nicht über die gleichen Anschlüsse und Stecker wie neuere Geräte. Zudem gibt es Geräte, die nicht ohne passenden Adapter mit anderen Geräten kompatibel sind. Liegt also z. B. ein passender Adapter nicht vor, so kann ein Laptop, der mit allen wichtigen Daten für eine Besprechung vorbereitet wurde, nicht an einen Beamer angeschlossen werden. Darüber hinaus können Versuche, die IT-Systeme dennoch zu verbinden, zu Schäden an den Geräten oder den gespeicherten Daten führen.

### 2.3 Gefährdung durch Besucher

Es ist nicht einfach, eigene Mitarbeiter ausreichend für den richtigen Umgang mit schützenswerten Informationen und IT-Systemen zu sensibilisieren. Im Gegensatz zu internen Mitarbeitern kann bei Besuchern grundsätzlich nicht vorausgesetzt werden, dass sie mit den ihnen zugänglichen Informationen und der Informationstechnik entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese Vorgaben in der Regel nicht kennen. Sind die eigenen Mitarbeiter unachtsam, können Besucher generell an vertrauliche Informationen gelangen. Ebenso kann dies aus Unwissenheit geschehen, wenn sich Besucher beispielsweise auf dem Weg zur Toilette in der Türe irren und ein Mitarbeiterbüro betreten, an dessen Whiteboard vertrauliche Informationen stehen. Besucher können auch vorsätzlich Geräte zerstören oder beschädigen, um an vertrauliche Informationen zu gelangen.

### 2.4 Fliegende Verkabelung

In Besprechungs-, Veranstaltungs- und Schulungsräumen wechseln häufig sowohl die Benutzer als auch die Art, wie die Räume genutzt werden. Dadurch wird mitunter die Geräteausstattung und damit auch die Verkabelung in diesen Räumen permanent geändert. Kabel können somit, je nach Lage der Anschlusspunkte im Raum (Steckdosen der Stromversorgung und des Datennetzes) übergangsweise quer durch den Raum, auch über Verkehrswege hinweg, verlegt werden. Nicht nur Personen werden durch diese Stolperfallen gefährdet, auch IT-Systeme können beschädigt werden, wenn Personen die „fliegenden“ Kabel mit sich reißen.

### 2.5 Diebstahl

Wenn die in einem Besprechungsraum teils stationär verbauten Datenträger, IT-Systeme, Zubehör,

Software oder Daten gestohlen werden, entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes. Andererseits kann der Besprechungsraum aufgrund mangelnder Verfügbarkeit der Geräte anschließend nur eingeschränkt genutzt werden. Dies verursacht möglicherweise Engpässe bei der Raumbelegung. Darüber hinaus können vertrauliche Informationen gestohlen, missbraucht oder weitergegeben werden.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht zu transportieren sind. Sind die Besprechungs-, Veranstaltungs- und Schulungsräume nicht beaufsichtigt oder die IT-Systeme nicht ausreichend gesichert, kann die Technik dementsprechend schnell und unauffällig entwendet werden. Dies gilt ganz besonders, wenn beispielsweise in Besprechungspausen die Räumlichkeiten nicht verschlossen werden.

## 2.6 Vertraulichkeitsverlust schützenswerter Informationen

Durch technisches Versagen, Unachtsamkeit, Unwissen und auch durch vorsätzliche Handlungen können vertrauliche Informationen offengelegt werden. Dabei können diese Informationen an unterschiedlichen Stellen vorliegen, z. B. auf Speichermedien innerhalb von IT-Systemen (wie Festplatten), auf austauschbaren Speichermedien (wie USB-Sticks oder optische Medien), in gedruckter Form auf Papier sowie auf Whiteboards oder Flipcharts. Werden Informationen unberechtigt gelesen oder preisgegeben, kann das schwerwiegende Folgen für die Institution haben, beispielsweise Verstöße gegen Gesetze, Wettbewerbsnachteile oder finanzielle Auswirkungen.

## 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* aufgeführt. Grundsätzlich ist die Zentrale Verwaltung für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Zentrale Verwaltung
Weitere Zuständigkeiten	Mitarbeiter, IT-Betrieb, Haustechnik

### 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* vorrangig erfüllt werden:

#### INF.10.A1 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen [Haustechnik, IT-Betrieb] (B)

In den Räumen vorhandene Gerätschaften MÜSSEN angemessen gegen Diebstahl gesichert werden. Zudem MUSS festgelegt werden, wer die in den Räumen dauerhaft vorhandenen IT- und sonstigen Systeme administriert. Es MUSS auch festgelegt werden, ob und unter welchen Bedingungen Besucher mitgebrachte IT-Systeme verwenden dürfen. Weiterhin MUSS festgelegt werden, ob und auf welche Netzzugänge und TK-Schnittstellen Besucher zugreifen dürfen.

#### INF.10.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

### **INF.10.A3 Geschlossene Fenster und Türen [Mitarbeiter] (B)**

Die Fenster der Besprechungs-, Veranstaltungs- und Schulungsräume MÜSSEN beim Verlassen verschlossen werden. Bei Räumlichkeiten, in denen sich IT-Systeme oder schützenswerte Informationen befinden, MÜSSEN die Türen beim Verlassen abgeschlossen werden. Zusätzlich MUSS regelmäßig geprüft werden, ob die Fenster und Türen nach Verlassen der Räume verschlossen wurden. Ebenso MUSS darauf geachtet werden, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden.

## **3.2 Standard-Anforderungen**

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume*. Sie SOLLTEN grundsätzlich erfüllt werden.

### **INF.10.A4 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen (S)**

Bei der Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen SOLLTE besonders die Lage der Räume berücksichtigt werden. Insbesondere Räumlichkeiten, die oft zusammen mit oder ausschließlich von Besuchern genutzt werden, SOLLTEN NICHT in Gebäudeteilen liegen, in deren Nähe regelmäßig vertrauliche Informationen bearbeitet werden. Es SOLLTE für jeden Raum festgelegt werden, wie vertraulich die Informationen sein dürfen, die dort besprochen oder verarbeitet werden.

### **INF.10.A5 Fliegende Verkabelung (S)**

Die Stromanschlüsse SOLLTEN sich dort befinden, wo Beamer, Laptops oder andere Verbraucher aufgestellt werden. Verkabelungen, die über den Boden verlaufen, SOLLTEN geeignet abgedeckt werden.

### **INF.10.A6 Einrichtung sicherer Netzzugänge [IT-Betrieb] (S)**

Es SOLLTE sichergestellt werden, dass mitgebrachte IT-Systeme nicht über das Datennetz mit internen IT-Systemen der Institution verbunden werden können. Auf das LAN der Institution SOLLTEN ausschließlich dafür vorgesehene IT-Systeme zugreifen können. Ein Datennetz für Besucher SOLLTE vom LAN der Institution getrennt werden. Netzzugänge SOLLTEN so eingerichtet sein, dass verhindert wird, dass Dritte den internen Datenaustausch mitlesen können. Netzanschlüsse in Besprechungs-, Veranstaltungs- oder Schulungsräumen SOLLTEN abgesichert werden. Es SOLLTE verhindert werden, dass IT-Systeme in Besprechungs-, Veranstaltungs- und Schulungsräumen gleichzeitig eine Verbindung zum Intranet und zum Internet aufbauen können.

Außerdem SOLLTE die Stromversorgung aus einer Unterverteilung heraus getrennt von anderen Räumen aufgebaut werden.

### **INF.10.A7 Sichere Konfiguration von Schulungs- und Präsentationsrechnern [IT-Betrieb] (S)**

Dedizierte Schulungs- und Präsentationsrechner SOLLTEN mit einer Minimalkonfiguration versehen werden. Es SOLLTE festgelegt sein, welche Anwendungen auf Schulungs- und Präsentationsrechnern in der jeweiligen Veranstaltung genutzt werden können. Die Schulungs- und Präsentationsrechner SOLLTEN nur an ein separates, vom LAN der Institution getrenntes Datennetz angeschlossen werden.

### **INF.10.A8 Erstellung eines Nutzungsnachweises für Räume (S)**

Je nach Nutzungsart der Besprechungs-, Veranstaltungs- und Schulungsräume SOLLTE ersichtlich sein, wer die Räume zu welchem Zeitpunkt genutzt hat. Für Räumlichkeiten, in denen Schulungen an IT-Systemen oder besonders vertrauliche Besprechungen durchgeführt werden, SOLLTEN ebenfalls Nutzungsnachweise erbracht werden. Es SOLLTE überlegt werden, für Räumlichkeiten, die für jeden Mitarbeiter zugänglich sind, ebenfalls entsprechende Nutzungsnachweise einzuführen.

## **3.3 Anforderungen bei erhöhtem Schutzbedarf**

Im Folgenden sind für den Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume*

exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

**INF.10.A9 Zurücksetzen von Schulungs- und Präsentationsrechnern [IT-Betrieb] (H)**

Es SOLLTE ein Verfahren festgelegt werden, um Schulungs- und Präsentationsrechner nach der Nutzung auf einen vorher definierten Zustand zurückzusetzen. Durch Benutzer vorgenommene Änderungen SOLLTEN dabei vollständig entfernt werden.

**INF.10.A10 Mitführverbot von Mobiltelefonen (H)**

Mobiltelefone SOLLTEN NICHT zu vertraulichen Besprechungen und Gesprächen mitgeführt werden. Falls erforderlich, SOLLTE dies durch Mobilfunk-Detektoren überprüft werden.

## 4 Weiterführende Informationen

### 4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.11 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden und Räumen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel CF19 Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden und Räumen.

Das Deutsche Institut für Normung macht in seiner Norm DIN EN 1627:2011-09 Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

## 5 Anlage: Kreuzreferenztablelle zu elementaren Gefährdungen

Die Kreuzreferenztablelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tablelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein INF.10 *Besprechungs-, Veranstaltungs- und Schulungsräume* von Bedeutung.

- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.21 Manipulation von Hard- oder Software
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.41 Sabotage
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust