Bundesamt
für Sicherheit in der
Informationstechnik

INF.7 Büroarbeitsplatz

1. Beschreibung

1.1. Einleitung

Ein Büroraum ist der Bereich innerhalb einer Institution, in dem sich ein, eine oder mehrere Mitarbeitende aufhalten, um dort ihre Aufgaben zu erfüllen. In diesem Baustein werden die typischen Gefährdungen und Anforderungen bezüglich der Informationssicherheit für einen Büroraum beschrieben.

1.2. Zielsetzung

Ziel des Bausteins ist der Schutz der Informationen, die in Büroräumen bearbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein INF.7 *Büroarbeitsplatz* ist auf jeden Raum im Informationsverbund anzuwenden, der als Büroarbeitsplatz genutzt wird.

Dieser Baustein betrachtet technische und nichttechnische Sicherheitsanforderungen für Büroräume. Empfehlungen, wie die IT-Systeme in diesen Räumen konfiguriert und abgesichert werden können, werden in diesem Baustein nicht behandelt. Hinweise dafür sind unter anderem im Baustein SYS.2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen Bausteinen zu finden.

Anforderungen an Gebäude im Allgemeinen sind nicht Teil dieses Bausteins. Diese sind im Baustein INF.1 *Allgemeines Gebäude* zu finden, der immer auf Räume und Gebäude anzuwenden ist. Auch auf die Verkabelung von Büroräumen wird nicht eingegangen. Dazu muss der Baustein INF.12 *Verkabelung* betrachtet werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein INF.7 *Büroarbeitsplatz* von besonderer Bedeutung.

2.1. Unbefugter Zutritt

Fehlen Zutrittskontrollen oder sind diese unzureichend, können unberechtigte Personen einen Büroraum betreten und schützenswerte Daten entwenden, Geräte stehlen oder sie manipulieren. Dadurch kann die Verfügbarkeit, Vertraulichkeit oder Integrität von Geräten und Informationen beeinträchtigt werden. Selbst wenn keine unmittelbaren Schäden erkennbar sind, kann der Betriebsablauf gestört werden. Beispielsweise muss untersucht werden, wie ein solcher Vorfall möglich war, ob Schäden aufgetreten sind oder Manipulationen vorgenommen wurden.

2.2. Beeinträchtigung durch ungünstige Arbeitsbedingungen

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Büroraum oder ein ungünstiges Arbeitsumfeld sind problematisch. Beides kann dazu führen, dass Mitarbeitende dort nicht ungestört arbeiten oder die verwendete IT nicht oder nicht optimal benutzen können. Störungen können Lärm, starker Kundschaftsverkehr, eine ungünstige Beleuchtung oder eine schlechte Belüftung sein. Dadurch können Arbeitsabläufe und das Potential der Mitarbeitenden eingeschränkt werden. Es können sich bei der Arbeit auch Fehler einschleichen, wodurch die Integrität von Daten vermindert werden kann.

2.3. Manipulationen durch Reinigungs- und Fremdpersonal oder Besuchende

Bei kleineren bzw. kurzen Besprechungen ist es meist effizienter, den Besuch im Büro zu empfangen. Dabei könnte jedoch der Besuch, ebenso wie auch Reinigungs- und Fremdpersonal, auf verschiedene Art und Weise interne Informationen einsehen, Geschäftsprozesse gefährden und IT-Systeme manipulieren. Angefangen von der unsachgemäßen Behandlung der technischen Einrichtungen über den Versuch des „Spielens“ an IT-Systemen bis zum Diebstahl von Unterlagen oder IT-Komponenten ist vieles möglich. So kann beispielsweise vom Reinigungspersonal versehentlich eine Steckverbindung gelöst werden oder Wasser in die IT gelangen. Auch können Unterlagen verlegt oder sogar mit dem Abfall entsorgt werden.

2.4. Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software im Büroraum

Angreifende können aus unterschiedlichen Gründen heraus versuchen, IT-Systeme, Zubehör und andere Datenträger zu manipulieren oder zu zerstören. Die Angriffe sind umso wirkungsvoller, je später sie von Mitarbeitenden oder der Institution selbst entdeckt werden, je umfassender die Kenntnisse der Täter und je tiefgreifender die Folgen für einen Arbeitsvorgang sind. Es könnten etwa unerlaubt schützenswerte Daten der Mitarbeitenden eingesehen werden. Auch könnten Datenträger oder IT-Systeme zerstört werden. Erhebliche Ausfallzeiten und Prozesseinschränkungen könnten die Folge sein.

2.5. Diebstahl

Da IT-Geräte immer handlicher werden, ist es umso leichter, sie unbemerkt in die Tasche zu stecken. Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Informationen entstehen einerseits Kosten für die Wiederbeschaffung. Aber auch für die Wiederherstellung eines arbeitsfähigen Zustandes sind Ressourcen nötig. Auf der anderen Seite können auch Verluste aufgrund mangelnder Verfügbarkeit entstehen. Darüber hinaus könnte die Person, die die IT-Geräte entwendet hat, vertrauliche Information einsehen und offenlegen. Dadurch können weitere Schäden entstehen. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des IT-Gerätes.

Gestohlen werden neben teuren IT-Systemen häufig auch mobile Endgeräte, die unauffällig und leicht transportiert werden können. Wenn die Büroräume nicht verschlossen, nicht beaufsichtigt oder die IT-

Systeme nicht ausreichend gesichert sind, kann die Technik dementsprechend schnell und unauffällig entwendet werden.

2.6. Fliegende Verkabelung

Je nachdem, wo die Anschlusspunkte der Steckdosen, der Stromversorgung und des Datennetzes im Büroraum liegen, könnten Kabel quer durch den Raum verlegt werden, auch über Verkehrswege hinweg. Solche „fliegenden" Kabel sind nicht nur Stolperfallen, an denen sich Personen verletzen können. Wenn Personen daran hängen bleiben, können auch IT-Geräte beschädigt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.7 *Büroarbeitsplatz* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Mitarbeitende, Zentrale Verwaltung, Haustechnik, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

INF.7.A1 Geeignete Auswahl und Nutzung eines Büroraumes (B) [Vorgesetzte]

Es DÜRFEN NUR geeignete Räume als Büroräume genutzt werden. Die Büroräume MÜSSEN für den Schutzbedarf bzw. das Schutzniveau der dort verarbeiteten Informationen angemessen ausgewählt und ausgestattet sein. Büroräume mit Publikumsverkehr DÜRFEN NICHT in sicherheitsrelevanten Bereichen liegen. Für den Arbeitsplatz und für die Einrichtung eines Büroraumes MUSS die Arbeitsstättenverordnung umgesetzt werden.

INF.7.A2 Geschlossene Fenster und abgeschlossene Türen (B) [Mitarbeitende, Haustechnik]

Wenn Mitarbeitende ihre Büroräume verlassen, SOLLTEN alle Fenster geschlossen werden. Befinden sich vertrauliche Informationen in dem Büroraum, MÜSSEN beim Verlassen die Türen abgeschlossen werden. Dies SOLLTE insbesondere in Bereichen mit Publikumsverkehr beachtet werden. Die entsprechenden Vorgaben SOLLTEN in einer geeigneten Anweisung festgehalten werden. Alle Mitarbeitenden SOLLTEN dazu verpflichtet werden, der Anweisung nachzukommen. Zusätzlich MUSS regelmäßig geprüft werden, ob beim Verlassen des Büroraums die Fenster geschlossen und, wenn notwendig, die Türen abgeschlossen werden. 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

INF.7.A3 Fliegende Verkabelung (S)

Die Stromanschlüsse und Zugänge zum Datennetz im Büroraum SOLLTEN sich dort befinden, wo die IT-Geräte aufgestellt sind. Verkabelungen, die über den Boden verlaufen, SOLLTEN geeignet abgedeckt werden.

INF.7.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

INF.7.A5 Ergonomischer Arbeitsplatz (S) [Zentrale Verwaltung, Vorgesetzte]

Die Arbeitsplätze aller Mitarbeitenden SOLLTEN ergonomisch eingerichtet sein. Vor allem die Bildschirme SOLLTEN so aufgestellt werden, dass ein ergonomisches und ungestörtes Arbeiten möglich ist. Dabei SOLLTE beachtet werden, dass Bildschirme nicht durch Unbefugte eingesehen werden können. Die Bildschirmarbeitsschutzverordnung (BildscharbV) SOLLTE umgesetzt werden. Alle Arbeitsplätze SOLLTEN für eine möglichst fehlerfreie Bedienung der IT individuell verstellbar sein.

INF.7.A6 Aufgeräumter Arbeitsplatz (S) [Mitarbeitende, Vorgesetzte]

Alle Mitarbeitenden SOLLTEN dazu angehalten werden, seinen Arbeitsplatz aufgeräumt zu hinterlassen. Die Mitarbeitenden SOLLTEN dafür sorgen, dass Unbefugte keine vertraulichen Informationen einsehen können. Alle Mitarbeitenden SOLLTEN ihre Arbeitsplätze sorgfältig überprüfen und sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind. Vorgesetzte SOLLTEN Arbeitsplätze sporadisch daraufhin überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind.

INF.7.A7 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger (S) [Mitarbeitende, Haustechnik]

Die Mitarbeitenden SOLLTEN angewiesen werden, vertrauliche Dokumente und Datenträger verschlossen aufzubewahren, wenn sie nicht verwendet werden. Dafür SOLLTEN geeignete Behältnisse in den Büroräumen oder in deren Umfeld aufgestellt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

INF.7.A8 Einsatz von Diebstahlsicherungen (H) [Mitarbeitende]

Wenn der Zutritt zu den Räumen nicht geeignet beschränkt werden kann, SOLLTEN für alle IT-Systeme Diebstahlsicherungen eingesetzt werden. In Bereichen mit Publikumsverkehr SOLLTEN Diebstahlsicherungen benutzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

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 1627:2021-11“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Das Bundesministerium für Arbeit und Soziales macht in seiner Arbeitsstättenverordnung Vorgaben zum Einrichten und Betreiben von Arbeitsstätten in Bezug auf die Sicherheit und den Schutz der Gesundheit von Beschäftigten.