Bundesamt
für Sicherheit in der
Informationstechnik

INF.8 Häuslicher Arbeitsplatz

1. Beschreibung

1.1. Einleitung

Telearbeitende, freie Mitarbeitende oder Selbstständige arbeiten typischerweise von häuslichen Arbeitsplätzen aus. Im Gegensatz zum Arbeitsplatz im Büro nutzen diese Mitarbeitenden einen Arbeitsplatz in der eigenen Immobilie. Dabei muss ermöglicht werden, dass die berufliche Umgebung hinreichend von der privaten getrennt ist. Wenn Mitarbeitende häusliche Arbeitsplätze dauerhaft benutzen, müssen zudem diverse rechtliche Anforderungen erfüllt sein, beispielsweise müssen die Arbeitsplätze arbeitsmedizinischen und ergonomischen Bestimmungen entsprechen.

Bei einem häuslichen Arbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausgesetzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist. So ist z. B. der Arbeitsplatz oft auch für Besuch oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist.

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie sich die Infrastruktur eines häuslichen Arbeitsplatzes sicher aufbauen und betreiben lässt. Kernziel des Bausteins ist der Schutz der Informationen der Institution am häuslichen Arbeitsplatz.

1.3. Abgrenzung und Modellierung

Der Baustein INF.8 *Häuslicher Arbeitsplatz* ist für alle Räume anzuwenden, die als Telearbeitsplatz genutzt werden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und zu erfüllen sind, um den Gefährdungen für einen häuslichen Arbeitsplatz entgegenwirken zu können. Dabei werden jedoch nur spezifische Anforderungen an die Infrastruktur für einen ortsfesten Arbeitsplatz mit Zugang durch Dritte definiert. Sicherheitsanforderungen für die eingesetzten IT-Systeme, z. B. Clients und Multifunktionsgeräte und insbesondere für die technischen Anteile der Telearbeit, z. B. Kommunikationsverbindungen, sind dagegen nicht Gegenstand des vorliegenden Bausteins. Sie werden im Baustein OPS.1.2.4 *Telearbeit* bzw. in den jeweiligen systemspezifischen Bausteinen beschrieben.

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.8 *Häuslicher Arbeitsplatz* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Regelungen für den häuslichen Arbeitsplatz

Da ein häuslicher Arbeitsplatz außerhalb der Institution liegt, sind die Mitarbeitenden dort weitgehend auf sich allein gestellt. Dadurch können durch fehlende oder unzureichende Regelungen für das häusliche Arbeitsplatzumfeld IT-Probleme mit höheren Ausfallzeiten entstehen. Wenn IT-Probleme nicht per Fernadministration geklärt werden können, muss beispielsweise eine Person vom IT-Betrieb aus der Institution erst zum häuslichen Arbeitsplatz fahren, um dort die Probleme zu beseitigen. Wenn der Umgang mit internen und vertraulichen Informationen am häuslichen Arbeitsplatz nicht nachvollziehbar geregelt ist, könnten Mitarbeitende solche Informationen falsch aufbewahren. Wenn nicht verhindert werden kann, dass Informationen ausgespäht oder modifiziert werden, kann die Vertraulichkeit und Integrität der Informationen gefährdet sein.

2.2. Unbefugter Zutritt zu schutzbedürftigen Räumen des häuslichen Arbeitsplatzes

Räume eines häuslichen Arbeitsplatzes, in denen schutzbedürftige Informationen aufbewahrt und weiterverarbeitet werden oder in denen schutzbedürftige Geräte aufbewahrt oder betrieben werden, werden dadurch zu schutzbedürftigen Räumen. Wenn unbefugte Personen diese Räume unbeaufsichtigt betreten können, ist die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten und Informationen erheblich gefährdet.

Beispiele:

- Ein Heimarbeitsplatz befindet sich zwar in einem separaten Arbeitszimmer, ist aber nicht konsequent abgeschlossen. Als kleine Kinder kurz unbeaufsichtigt waren, spielten sie in dem nicht verschlossenen Arbeitszimmer. Dabei wurden wichtige Dokumente als Malgrundlage verwendet.
- Als eine Person am häuslichen Arbeitsplatz in eine Projektarbeit vertieft war, traf überraschend Besuch ein. Während die Person in der Küche Kaffee kochte, wollte der Besuch am nicht gesperrten Client schnell etwas im Internet recherchieren und hat diesen dabei versehentlich mit Schadsoftware infiziert.

2.3. Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen am häuslichen Arbeitsplatz

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter häuslicher Arbeitsplatz oder ein ungünstiges Arbeitsumfeld können dazu führen, dass dort nicht ungestört gearbeitet werden kann. Auch die verwendete IT kann möglicherweise nicht oder nicht optimal benutzt werden. Ungünstig auswirken können sich etwa Lärm, Störungen durch Familienmitglieder sowie eine schlechte Beleuchtung oder Belüftung. Dadurch werden Arbeitsabläufe und Potenziale der Mitarbeitenden eingeschränkt. Es könnten sich bei der Arbeit auch Fehler einschleichen. Außerdem kann der Schutz der Integrität von Daten vermindert werden.

2.4. Ungesicherter Akten- und Datenträgertransport

Wenn Dokumente, Datenträger oder Akten zwischen der Institution und dem häuslichen Arbeitsplatz transportiert werden, können diese Daten und Informationen verlorengehen. Auch könnten sie von unbefugten Dritten entwendet, gelesen oder manipuliert werden. Der Akten- und Datenträgertransport kann auf verschiedene Arten unzureichend gesichert sein:

- Werden Unikate transportiert und fehlt ein entsprechendes Backup, können Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verlorengeht.
- Fallen unverschlüsselte Datenträger in falsche Hände, kann das zu einem schwerwiegenden Verlust der Vertraulichkeit führen.
- Wenn unterwegs kein ausreichender Zugriffsschutz vorhanden ist, können Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

2.5. Ungeeignete Entsorgung der Datenträger und Dokumente

Ist es am häuslichen Arbeitsplatz nicht möglich, Datenträger und Dokumente in geeigneter Weise zu entsorgen, könnten sie einfach in den Hausmüll geworfen werden. Hieraus können jedoch wertvolle Informationen gewonnen werden, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zur Existenzgefährdung der Institution, z. B. wenn dadurch wichtige Aufträge nicht zustande kommen oder geschäftliche Partnerschaften scheitern.

2.6. Manipulation oder Zerstörung von IT, Zubehör, Informationen und Software am häuslichen Arbeitsplatz

IT-Geräte, Zubehör, Informationen und Software, die am häuslichen Arbeitsplatz benutzt werden, können unter Umständen einfacher manipuliert oder zerstört werden als in der Institution. Der häusliche Arbeitsplatz ist oft für Angehörige und Besuch der Familie zugänglich. Auch sind hier die zentralen Schutzmaßnahmen der Institution nicht vorhanden, zum Beispiel Pfortendienste. Wenn IT-Geräte, Zubehör, Informationen oder Software manipuliert oder zerstört werden, sind Mitarbeitende am häuslichen Arbeitsplatz oft nur noch eingeschränkt arbeitsfähig. Des Weiteren müssen womöglich zerstörte IT-Komponenten, Informationen und Softwarelösungen ersetzt werden, was sowohl finanzielle als auch zeitliche Ressourcen erfordert.

2.7. Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Der häusliche Arbeitsplatz ist meistens nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder in einer Behörde. Durch aufwendige Vorkehrungen wie z. B. Sicherheitstüren oder einem Pfortendienst ist dort die Gefahr, dass jemand unbefugt in das Gebäude eindringt, weitaus geringer als bei einem Privathaus. Bei einem Einbruch werden meistens vorrangig Gegenstände gestohlen, die schnell und einfach verkauft werden können. Dabei kann auch dienstliche IT gestohlen werden. Die auf den entwendeten dienstlichen IT-Systemen vorhandenen Informationen besitzen aber oft einen höheren Wert als die IT-Systeme selbst. Dritte könnten versuchen, durch Erpressung oder Weitergabe der Daten an Konkurrenzunternehmen einen höheren Gewinn als durch den Verkauf der Hardware zu erzielen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins INF.8 *Häuslicher Arbeitsplatz* 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	Mitarbeitende
Weitere Zuständigkeiten	Keine

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.8.A1 Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz (B)

Dienstliche Unterlagen und Datenträger MÜSSEN am häuslichen Arbeitsplatz so aufbewahrt werden, dass keine unbefugten Personen darauf zugreifen können. Daher MÜSSEN ausreichend verschließbare Behältnisse (z. B. abschließbare Rollcontainer oder Schränke) vorhanden sein. Alle Mitarbeitenden MÜSSEN ihre Arbeitsplätze aufgeräumt hinterlassen und sicherstellen, dass keine vertraulichen Informationen frei zugänglich sind.

INF.8.A2 Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz (B)

Es MUSS geregelt werden, welche Datenträger und Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen. Generell MÜSSEN Datenträger und andere Unterlagen sicher transportiert werden. Diese Regelungen MÜSSEN den Mitarbeitenden in geeigneter Weise bekanntgegeben werden.

INF.8.A3 Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz (B)

Den Mitarbeitenden MUSS mitgeteilt werden, welche Regelungen und Maßnahmen zum Einbruchs- und Zutrittsschutz zu beachten sind. So MUSS darauf hingewiesen werden, Fenster zu schließen und Türen abzuschließen, wenn der häusliche Arbeitsplatz nicht besetzt ist.

Es MUSS sichergestellt werden, dass unbefugte Personen zu keiner Zeit den häuslichen Arbeitsplatz betreten und auf dienstliche IT und Unterlagen zugreifen können. Diese Maßnahmen MÜSSEN in sinnvollen zeitlichen Abständen überprüft werden, mindestens aber, wenn sich die häuslichen Verhältnisse ändern.

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.8.A4 Geeignete Einrichtung des häuslichen Arbeitsplatzes (S)

Der häusliche Arbeitsplatz SOLLTE durch eine geeignete Raumaufteilung von den privaten Bereichen der Wohnung getrennt sein. Der häusliche Arbeitsplatz SOLLTE mit Büromöbeln eingerichtet sein, die ergonomischen Anforderungen entsprechen.

Ebenso SOLLTE der häusliche Arbeitsplatz durch geeignete technische Sicherungsmaßnahmen vor Einbrüchen geschützt werden. Die Schutzmaßnahmen SOLLTEN an die örtlichen Gegebenheiten und den vorliegenden Schutzbedarf angepasst sein.

INF.8.A5 Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz (S)

Vertrauliche Informationen SOLLTEN sicher entsorgt werden. In einer speziellen Sicherheitsrichtlinie SOLLTE daher geregelt werden, wie schutzbedürftiges Material zu beseitigen ist. Es SOLLTEN die dafür benötigten Entsorgungsmöglichkeiten verfügbar sein.

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.8.A6 Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am häuslichen Arbeitsplatz (H)

Wenn Informationen mit erhöhtem Schutzbedarf bearbeitet werden, SOLLTE überlegt werden, von einem häuslichen Arbeitsplatz ganz abzusehen. Anderenfalls SOLLTE der häusliche Arbeitsplatz durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt 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 Deutsche Institut für Normung macht in seiner Norm „DIN EN 1627:2011-09“ Vorgaben zur physischen Sicherheit von Gebäuden und Räumen.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-53 zu „Assessing Security and Privacy Controls for Federal Information Systems and Organizations“ veröffentlicht und macht im Appendix F-PS Vorgaben zur physischen Sicherheit und Umgebungssicherheit von Gebäuden.