SYS.3: Mobile Devices

SYS.3.1: Laptops

1 Beschreibung

1.1 Einleitung

Ein Laptop (auch Notebook genannt) ist ein PC, der mobil genutzt werden kann. Er hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm, ist über Akkus zeitweise unabhängig von einer externen Stromversorgung und besteht oft aus speziell für den mobilen Einsatz konzipierten Hardware-Komponenten. Laptops sind in den meisten Institutionen verbreitet und ersetzen häufig den klassischen Desktop-PC.

Laptops werden in der Regel mit verbreiteten Desktop-Betriebssystemen wie Microsoft Windows, Apple macOS oder Linux betrieben. Die Grenzen zu Tablets und ähnlichen Geräten sind heutzutage fließend. So gibt es Tablets mit Desktop-Betriebssystemen wie Windows 10, aber auch Tastaturzubehör für Mobilgeräte wie iPads mit iPadOS, die so als Laptops genutzt werden können.

Da Laptops häufig auch mobil genutzt werden, sind sie oft nicht permanent am LAN der Institution angeschlossen. Stattdessen können sie sich in der Regel per Virtual Private Network (VPN) z. B. über das Internet mit dem Netz der Institution verbinden. Auch die Infrastruktur einer klassischen Büroumgebung, die kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschützte Bereiche bietet, kann beim mobilen Einsatz von Laptops nicht vorausgesetzt werden.

1.2 Zielsetzung

Ziel des Bausteins ist es, Institutionen einen sicheren Einsatz von Laptops zu ermöglichen sowie für die spezifischen Gefährdungen dieser Geräteklasse zu sensibilisieren.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.3.1 *Laptops* ist auf alle Laptops anzuwenden, die mobil oder stationär genutzt werden.

Wie bei allen IT-Systemen müssen auch bei Laptops die Betriebssystem- und Software-Komponenten sorgfältig ausgewählt und installiert werden. Die hier zu erfüllenden Anforderungen sind abhängig vom Betriebssystem des Laptops und werden daher in den Client-spezifischen Bausteinen beschrieben, beispielsweise SYS.2.2.3 *Clients unter Windows 10,* SYS 2.3 *Clients unter Linux und Unix* oder SYS.2.4 *Clients unter macOS*. Ebenso sind Anforderungen, die für alle Arten von Clients gelten, nicht Bestandteil dieses Bausteins. Diese sind im Baustein SYS.2.1 *Allgemeiner Client* zu finden.

Auch wird in diesem Baustein nicht behandelt, wie die jeweilige Datenübertragung einzurichten ist, wie z. B. die WLAN-Konfiguration (siehe NET.2.2 *WLAN-Nutzung*) oder eine VPN-Anbindung (siehe NET.3.3 *VPN*).

Da Laptops oft längere Zeit außerhalb einer Institution eingesetzt werden, müssen sie besonders bei der Datensicherung berücksichtigt werden. Weiterführende Anforderungen dazu finden sich in Baustein CON.3 *Datensicherungskonzept*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.3.1 *Laptops* von besonderer Bedeutung:

2.1 Beeinträchtigung durch wechselnde Einsatzumgebung

Laptops werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch vielen Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen, ebenso Staub oder Feuchtigkeit. Bei Laptops besteht auch stets die Gefahr von Transportschäden. Außerdem kommunizieren Laptops vor allem unterwegs oft mit unbekannten IT-Systemen oder Netzen, was immer ein Gefährdungspotenzial für das eigene Gerät mit sich bringt. So können dabei beispielsweise Schadprogramme übertragen oder schützenswerte Informationen kopiert werden.

2.2 Diebstahl und Verlust von Laptops

Mitarbeiter nutzen ihre Laptops regelmäßig auch außerhalb der Institution. Die Geräte werden etwa in privaten Kraftfahrzeugen oder in öffentlichen Verkehrsmitteln transportiert, in fremden Büroräumen in Pausen zurückgelassen oder in Hotelzimmern unbewacht aufgestellt. Somit sind Laptops einem höheren Diebstahlrisiko ausgesetzt und können zudem leicht vergessen oder verloren werden. Kommt ein Laptop abhanden, entstehen Kosten und Aufwand für die Wiederbeschaffung. Nicht gesicherte Daten sind zudem verloren. Ebenso könnten Unbefugte auf schützenswerte Daten zugreifen, wodurch es zu weiteren Schäden kommen kann. Diese wiegen in vielen Fällen deutlich schwerer als der rein materielle Verlust des Laptops.

2.3 Ungeordneter Benutzerwechsel bei Laptops

Wenn Mitarbeiter nur in Ausnahmefällen mobile IT-Systeme benötigen, wie beispielsweise für selten durchgeführte Dienstreisen, ist es oft zweckmäßiger, nur wenige Laptops für viele Benutzer vorzuhalten. Diese können dann untereinander weitergereicht werden. Wird jedoch bei einem Benutzerwechsel der Laptop einfach an den nächsten Mitarbeiter übergeben, besteht die Gefahr, dass noch auf dem Gerät befindliche schutzbedürftige Daten weitergegeben werden. Außerdem ist es möglich, dass der Laptop mit Schadsoftware infiziert ist. Ohne eine geeignete Regelung kann schwer nachvollziehbar sein, wer den Laptop wann benutzt hat oder wer ihn zurzeit benutzt.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.1 *Laptops* aufgeführt. Grundsätzlich ist der IT-Betrieb 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 Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer, Beschaffungsstelle

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.1 *Laptops* vorrangig erfüllt werden:

SYS.3.1.A1 Regelungen zur mobilen Nutzung von Laptops (B)

Es MUSS klar geregelt werden, was Mitarbeiter bei der mobilen Nutzung von Laptops berücksichtigen müssen. Es MUSS insbesondere festgelegt werden, welche Laptops mobil genutzt werden dürfen, wer sie mitnehmen darf und welche grundlegenden Sicherheitsmaßnahmen dabei zu beachten sind. Die Benutzer MÜSSEN auf die Regelungen hingewiesen werden.

SYS.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.1.A3 Einsatz von Personal Firewalls (B)

Auf Laptops MUSS eine Personal Firewall aktiv sein, wenn sie außerhalb von Netzen der Institution eingesetzt werden. Die Filterregeln der Firewall MÜSSEN so restriktiv wie möglich sein. Sie MÜSSEN regelmäßig getestet werden. Die Personal Firewall MUSS so konfiguriert werden, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.

SYS.3.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.1.A9 Sicherer Fernzugriff mit Laptops (B)

Über öffentlich zugängliche Netze DÜRFEN die Benutzer NUR über über einen sicheren Kommunikationskanal auf das interne Netz der Institution zugreifen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.3.1 *Laptops*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.1.A6 Sicherheitsrichtlinien für Laptops (S)

Für Laptops SOLLTE eine Sicherheitsrichtlinie erstellt werden, die regelt, wie die Geräte benutzt werden dürfen. Die Benutzer SOLLTEN hinsichtlich des Schutzbedarfs von Laptops und der dort gespeicherten Daten sensibilisiert werden. Auch SOLLTEN sie auf die spezifischen Gefährdungen bzw. die entsprechenden Anforderungen für die Nutzung aufmerksam gemacht werden. Sie SOLLTEN außerdem darüber informiert werden, welche Art von Informationen sie auf Laptops verarbeiten dürfen.

SYS.3.1.A7 Geregelte Übergabe und Rücknahme eines Laptops [Benutzer] (S)

Wenn Laptops von verschiedenen Personen abwechselnd genutzt werden, SOLLTE geregelt werden, wie sie sicher an Mitarbeiter übergeben werden können. Auch SOLLTE geregelt werden, wie sie wieder sicher zurückzunehmen sind. Beim Benutzerwechsel eines Laptops SOLLTEN eventuell vorhandene schützenswerte Daten sicher gelöscht werden. Falls der Laptop nach dem Benutzerwechsel nicht neu aufgesetzt wird, SOLLTE sichergestellt sein, dass sich auf dem IT-System und allen damit verbundenen Datenträgern keine Schadsoftware befindet. Mit einem Laptop SOLLTE den Benutzern ein Merkblatt für den sicheren Umgang mit dem Gerät ausgehändigt werden.

SYS.3.1.A8 Sicherer Anschluss von Laptops an Datennetze [Benutzer] (S)

Es SOLLTE geregelt werden, wie Laptops sicher an eigene oder fremde Datennetze und an das Internet angeschlossen werden. Nur zugelassene Laptops SOLLTEN sich am internen Netz der Institution

anmelden können.

SYS.3.1.A10 Abgleich der Datenbestände von Laptops [Benutzer] (S)

Es SOLLTE geregelt werden, wie Daten von Laptops in den Informationsverbund der Institution übernommen werden. Wenn ein Synchronisationstool benutzt wird, SOLLTE sichergestellt sein, dass Synchronisationskonflikte aufgelöst werden können. Der Synchronisationsvorgang SOLLTE protokolliert werden. Außerdem SOLLTEN die Benutzer angewiesen werden, die Synchronisationsprotokolle zu prüfen.

SYS.3.1.A11 Sicherstellung der Energieversorgung von Laptops [Benutzer] (S)

Alle Benutzer SOLLTEN darüber informiert werden, wie sie die Energieversorgung von Laptops im mobilen Einsatz optimal sicherstellen können. Vorhandene Ersatzakkus SOLLTEN in geeigneten Hüllen gelagert und transportiert werden.

SYS.3.1.A12 Verlustmeldung für Laptops [Benutzer] (S)

Benutzer SOLLTEN umgehend melden, wenn ein Laptop verloren gegangen ist oder gestohlen wurde. Dafür SOLLTE es in der Institution klare Meldewege geben. Wenn verlorene Laptops wieder auftauchen, SOLLTE untersucht werden, ob sie eventuell manipuliert wurden. Die darauf eingesetzte Software inklusive des Betriebssystems SOLLTE komplett neu installiert werden.

SYS.3.1.A13 Verschlüsselung von Laptops (S)

In Laptops verbaute Datenträger wie Festplatten oder SSDs SOLLTEN verschlüsselt werden.

SYS.3.1.A14 Geeignete Aufbewahrung von Laptops [Benutzer] (S)

Alle Benutzer SOLLTEN darauf hingewiesen werden, wie Laptops außerhalb der Institution sicher aufzubewahren sind. Abhängig vom Schutzbedarf der darauf gespeicherten Daten SOLLTEN Laptops auch in den Räumen der Institution außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt werden.

SYS.3.1.A15 Geeignete Auswahl von Laptops [Beschaffungsstelle] (S)

Bevor Laptops beschafft werden, SOLLTEN die Zuständigen eine Anforderungsanalyse durchführen. Anhand der Ergebnisse SOLLTEN alle infrage kommenden Geräte bewertet werden. Die Beschaffungsentscheidung SOLLTE mit dem IT-Betrieb abgestimmt sein.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.3.1 *Laptops* 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.

SYS.3.1.A16 Zentrale Administration und Verwaltung von Laptops (H)

Es SOLLTE eine geeignete Regelung definiert werden, wie Laptops zentral zu administrieren und verwalten sind. Ein Tool zum zentralen Laptop-Management SOLLTE möglichst alle eingesetzten Betriebssysteme unterstützen.

SYS.3.1.A17 Sammelaufbewahrung von Laptops (H)

Nicht benutzte Laptops SOLLTEN in einem geeignet abgesicherten Raum vorgehalten werden. Der dafür genutzte Raum SOLLTE den Anforderungen aus INF.5 *Raum sowie Schrank für technische Infrastruktur* entsprechen.

SYS.3.1.A18 Einsatz von Diebstahl-Sicherungen (H)

Es SOLLTE geregelt werden, welche Diebstahlsicherungen für Laptops eingesetzt werden sollen. Bei mechanischen Sicherungen SOLLTE besonders auf ein gutes Schloss geachtet werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Für den Baustein SYS.3.1 *Laptops* sind keine weiterführenden Informationen vorhanden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle 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 SYS.3.1 *Laptops* von Bedeutung.

G 0.4 Verschmutzung, Staub, Korrosion

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen