Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2: Desktop-Systeme

# SYS.2.1: Allgemeiner Client

## 1 Beschreibung

### 1.1 Einleitung

Als „Allgemeiner Client“ wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt und nicht dazu dient, Server-Dienste bereitzustellen. Auf einem Client sollten mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können. Das IT-System verfügt in der Regel über Laufwerke und Anschlussmöglichkeiten für externe bzw. wechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte. Typischerweise ist ein solches IT-System in ein Client-Server-Netz eingebunden. Bei dem IT-System kann es sich beispielsweise um einen PC mit oder ohne Festplatte, um ein mobiles oder stationäres Gerät, aber auch um eine Linux-Workstation oder einen Apple Mac handeln.

### 1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf jeglicher Art von Clients, unabhängig vom verwendeten Betriebssystem, erstellt, gelesen, bearbeitet, gespeichert oder versendet werden.

### 1.3 Abgrenzung und Modellierung

Der Baustein SYS.2.1 *Allgemeiner Client* ist für alle Clients unabhängig vom konkreten Betriebssystem anzuwenden.

In der Regel werden Clients unter einem Betriebssystem ausgeführt, das jeweils eigene Sicherheitsmaßnahmen erfordert. Für verbreitete Client-Betriebssysteme sind spezifische Bausteine in der Schicht SYS.2 *Desktop-Systeme* vorhanden, die auf dem vorliegenden Baustein aufbauen und zusätzlich anzuwenden sind. Falls für eingesetzte Clients kein spezifischer Baustein existiert, müssen die Anforderungen des vorliegenden Bausteins geeignet angepasst und erweitert werden. Sicherheitsempfehlungen für mobile Endgeräte mit festem Betriebssystem, wie Smartphones oder Tablets, sind in der Schicht SYS.3 *Mobile Devices* zu finden.

Falls ein Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, LAN oder WLAN, müssen diese gemäß den Sicherheitsvorgaben der Institution so abgesichert werden, wie es in den entsprechenden Bausteinen beschrieben ist. Hierzu sind Anforderungen beispielsweise in SYS.4.5 *Wechseldatenträger* oder NET.2.2 *WLAN-Nutzung* zu finden.

Regelmäßig sind außerdem die Anforderungen des Baustein CON.3 *Datensicherungskonzept* für Clients zu berücksichtigen. Clients sind oft durch Schadsoftware gefährdet. Deswegen sind die Anforderungen des Bausteins OPS.1.1.4 *Schutz vor Schadprogrammen* bei Clients zu berücksichtigen.

# 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.2.1 *Allgemeiner Client* von besonderer Bedeutung:

## 2.1 Schadprogramme

Schadprogramme werden mit dem Ziel entwickelt, unerwünschte und schädliche Funktionen auf IT-Systemen auszuführen. Sie werden meist „heimlich" aktiv, d. h. ohne dass die Benutzer davon wissen oder darin einwilligen. Je nach Ausprägung bieten sie einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten mit vielen unterschiedlichen Funktionen. Unter anderem könnten sie gezielt Passwörter auslesen, IT-Systeme fernsteuern, Schutzsoftware deaktivieren, Daten ausspionieren oder verschlüsseln.

Clients sind besonders anfällig für Schadsoftware. Sie werden direkt von den Benutzern bedient und sind somit oft das Einfallstor für schädliche Inhalte jeglicher Art. Besuchen die Benutzer bösartige Webseiten, öffnen E-Mails mit schädlichem Inhalt von privaten Konten oder kopieren Schadsoftware über lokale Datenträger auf den Client, kann sich so die Schadsoftware über die Clients in das Netz der Institution verbreiten. Zentrale Schutzmechanismen, wie z. B. ein Virenschutz auf dem Datei- oder E-Mail-Server, können so oft umgangen werden.

## 2.2 Datenverlust durch lokale Datenhaltung

Trotz regelmäßiger, gegensätzlicher Empfehlung speichern viele Benutzer auch wichtige Daten ausschließlich lokal ab. Beispielsweise werden Daten häufig in lokalen Benutzerverzeichnissen abgelegt, statt auf einem zentralen Dateiserver. Auch E-Mails werden häufig nur lokal archiviert. So können etwa bei Hardwaredefekten leicht Daten verloren gehen. Werden für die Institution wichtige Daten zerstört oder verfälscht, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar ganz verhindert werden. Insgesamt kann der Verlust gespeicherter Daten neben einem Arbeitsausfall und den Kosten für eine Wiederbeschaffung auch zu langfristigen Konsequenzen wie beispielsweise Vertrauenseinbußen bei Kunden und Partnern sowie einem negativen Eindruck in der Öffentlichkeit führen. Durch die von den durch Datenverluste verursachten direkten und indirekten Schäden können Institutionen im Extremfall in ihrer Existenz bedroht sein.

Werden wichtige Daten ausschließlich lokal gehalten, können andere Benutzer außerdem nicht darauf zugreifen, etwa im Vertretungsfall bei Urlaub oder Krankheit.

Auch wenn grundsätzliche Vorgaben zur zentralen Speicherung eingehalten werden, werden oftmals zusätzlich lokale Kopien der zentral gespeicherten Daten angelegt. Dies führt nicht nur häufig zu inkonsistenten Versionsständen, sondern auch dazu, dass Daten entweder vorschnell oder nicht wie notwendig gelöscht werden.

## 2.3 Hardware-Defekte bei Client-Systemen

Anders als bei zentralen IT-Systemen wie Servern, arbeiten Client-Benutzer direkt am Endgerät. Dadurch könnten sie den Client unter Umständen gewollt oder ungewollt beschädigen. Beispielsweise könnten sie gegen auf dem Boden stehende IT-Systeme treten, über Kabel stolpern und damit Schnittstellen beschädigen oder Flüssigkeiten über Geräte verschütten. Gibt es keinen schnellen Ersatz, kann der Benutzer das IT-System bis zum Abschluss der Reparatur nicht für seine Arbeit einsetzen. Fällt ein mobiles Gerät wie ein Laptop unterwegs aus, kann die Arbeit oft erst nach der Rückkehr in die Institution fortgesetzt werden.

## 2.4 Unberechtigte IT-Nutzung

Die Identifikation und Authentisierung von Benutzern soll verhindern, dass ein Client unberechtigt verwendet wird. Aber auch IT-Systeme, bei denen sich Benutzer über Benutzer-IDs und Passwörter identifizieren und authentisieren müssen, können unberechtigt genutzt werden, wenn es einem

Angreifer gelingt, die Zugangsdaten auszuspähen oder zu erraten. Wird keine Bildschirmsperre aktiviert, kann der Client auch bei kurzzeitiger Abwesenheit unberechtigt genutzt werden.

### 2.5 Installation nicht benötigter Betriebssystemkomponenten und Applikationen

Bei der Installation eines Betriebssystems besteht in der Regel die Möglichkeit, optionale Software zu installieren. Auch im laufenden Betrieb wird regelmäßig Software installiert und getestet. Mit jeder weiteren Anwendung steigen nicht nur Rechen- und Speicherlast eines Clients an, sondern auch die Wahrscheinlichkeit für darin verborgene Schwachstellen. Nicht benötigte Software unterliegt außerdem häufig keinem regelmäßigen Patch-Management, sodass auch bekannte Sicherheitslücken nicht zeitnah geschlossen werden. Dadurch können Angreifer auch solche Schwachstellen ausnutzen, die schon lange bekannt sind.

### 2.6 Abhören von Räumen mittels Mikrofon und Kamera

Viele Clients verfügen über ein Mikrofon und eine Kamera. Diese können prinzipiell von jedem aktiviert und verwendet werden, der über entsprechende Zugriffsrechte verfügt, bei vernetzten Systemen auch von Externen. Werden diese Rechte nicht sorgfältig vergeben, können Unbefugte Mikrofon oder Kamera dazu missbrauchen, um über das Internet Räume abzuhören oder unbemerkt Besprechungen aufzuzeichnen. Hierzu gehören auch Intelligente Persönliche Assistenten (IPA) oder Sprachassistenten, die die Umgebung permanent abhören und nach Nennung eines geräteabhängigen Aktivierungsworts bestimmte Funktionen ausführen, wie Musik abspielen, Kontakte anrufen, die Beleuchtung steuern oder das Raumklima verändern. Werden die Gespräche z. B. von IPAs an Dritte übermittelt, könnten diese unter Umständen von Unbefugten abgehört werden. Die aufgezeichneten Gespräche könnten auch bei den Betreibern des IPA längerfristig abgespeichert und weiterverarbeitet werden.

### 2.7 Fehlerhafte Administration oder Nutzung von Geräten und Systemen

Moderne Client-Betriebssysteme sind sehr komplex. Daher können insbesondere Fehlkonfiguration von Komponenten die Sicherheit beeinträchtigen, sodass das IT-System fehlerhaft funktioniert oder kompromittiert werden kann. Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass Unbefugte auf das IT-System zugreifen. Wenn etwa durch Fehlkonfiguration der Authentisierungsmechanismen Benutzerkennungen und zugehörige Passwörter ausgespäht werden können, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.

Auch eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann die Sicherheit beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. So können beispielsweise zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Arbeitsplätze zu Sicherheitsvorfällen führen. Eine weitere Folge der fehlerhaften Bedienung von IT-Systemen oder Anwendungen kann das versehentlich Löschen oder Verändern von Daten sein. Dabei ist es ebenfalls möglich, dass vertrauliche Informationen in die Hände Dritter gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

## 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.1 *Allgemeiner Client* 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, Haustechnik |

## 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.2.1 *Allgemeiner Client* vorrangig erfüllt werden:

### SYS.2.1.A1 Sichere Benutzerauthentisierung (B)

Um den Client zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Benutzer MÜSSEN eine Bildschirmsperre verwenden, wenn sie den Client unbeaufsichtigt betreiben. Die Bildschirmsperre SOLLTE automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne keine Aktion durch den Benutzer durchgeführt wurde. Die Bildschirmsperre DARF NUR durch eine erfolgreiche Benutzerauthentisierung deaktiviert werden können. Die Benutzer SOLLTEN verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

### SYS.2.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

### SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B)

Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, SOLLTE mindestens täglich automatisch nach Updates gesucht und diese installiert werden.

### SYS.2.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

### SYS.2.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

### SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)

Abhängig vom installierten Betriebssystem und von anderen vorhandenen Schutzmechanismen des Clients MUSS geprüft werden, ob Schutzprogramme gegen Schadsoftware eingesetzt werden sollen. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein solcher Schutz notwendig ist, aus den Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums berücksichtigt werden.

Schutzprogramme auf den Clients MÜSSEN so konfiguriert sein, dass die Benutzer weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen noch die Schutzprogramme deaktivieren können.

Das Schutzprogramm MUSS nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Der gesamte Datenbestand eines Clients MUSS regelmäßig auf Schadsoftware geprüft werden. Wenn ein Client infiziert ist, MUSS im Offlinebetrieb untersucht werden, ob ein gefundenes Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

### SYS.2.1.A7 ENTFALLEN (B)

Diese Anforderung ist entfallen.

### SYS.2.1.A8 Absicherung des Bootvorgangs (B)

Der Startvorgang des IT-Systems („Booten“) MUSS gegen Manipulation abgesichert werden. Es MUSS

festgelegt werden, von welchen Medien gebootet werden darf. Es SOLLTE entschieden werden, ob und wie der Bootvorgang kryptografisch geschützt werden soll. Es MUSS sichergestellt werden, dass nur Administratoren die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können. NUR Administratoren DÜRFEN von wechselbaren oder externen Speichermedien booten können. Die Konfigurationseinstellungen des Bootvorgangs DÜRFEN NUR durch Administratoren verändert werden können. Alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden.

**SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen [Benutzer] (B)**

Es DÜRFEN NUR zwingend notwendige Cloud- und Online-Funktionen des Betriebssystems genutzt werden. Die notwendigen Cloud- und Online-Funktionen SOLLTEN dokumentiert werden. Die entsprechenden Einstellungen des Betriebssystems MÜSSEN auf Konformität mit den organisatorischen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. die Funktionen deaktiviert werden.

## 3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.2.1 *Allgemeiner Client*. Sie SOLLTEN grundsätzlich erfüllt werden.

**SYS.2.1.A9 Festlegung einer Sicherheitsrichtlinie für Clients (S)**

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an allgemeine Clients konkretisiert werden. Die Richtlinie SOLLTE allen Benutzern sowie allen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden.

**SYS.2.1.A10 Planung des Einsatzes von Clients (S)**

Es SOLLTE im Vorfeld geplant werden, wo und wie Clients eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die typischerweise direkt mit den Begriffen IT- oder Informationssicherheit in Verbindung gebracht werden, sondern auch betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

**SYS.2.1.A11 Beschaffung von Clients (S)**

Bevor Clients beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Die jeweiligen Hersteller von IT- und Betriebssystem SOLLTEN für den gesamten geplanten Nutzungszeitraum Patches für Schwachstellen zeitnah zur Verfügung stellen. Die zu beschaffenden Systeme SOLLTEN über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot und, sofern vorhanden, für das TPM verfügen, die eine Kontrolle durch den Eigentümer (Institution) gewährleistet und so den selbstverwalteten Betrieb von SecureBoot und des TPM ermöglicht.

**SYS.2.1.A12 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (S)**

Der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (z. B. durch das Betriebssystem speziell abgesicherte Speicherbereiche, Firmwarebereiche etc.) SOLLTE nur durch Benutzer mit administrativen Berechtigungen möglich sein. Die entsprechenden Einstellungen im BIOS bzw. der UEFI-Firmware SOLLTEN durch ein Passwort vor unberechtigten Veränderungen geschützt werden. Wird die Kontrolle über die Funktionen an das Betriebssystem delegiert, SOLLTEN auch dort nur Benutzer mit administrativen Berechtigungen auf die Funktionen zugreifen dürfen.

### SYS.2.1.A14 Updates und Patches für Firmware, Betriebssystem und Anwendungen (S)

Auf Betriebssysteme, die über ein Rolling-Release-Modell aktualisiert werden, SOLLTE verzichtet werden. Es SOLLTEN NUR Anwendungsprogramme ausgewählt und installiert werden, für die Support angeboten wird. Betriebssysteme, Anwendungsprogramme und Firmware, für die keine regelmäßigen Sicherheitsupdates angeboten werden, DÜRFEN NICHT eingesetzt werden.

### SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S)

Es SOLLTE festgelegt werden, welche Komponenten des Betriebssystems, welche Fachanwendungen und welche weiteren Tools installiert werden sollen. Die Installation und Konfiguration der IT-Systeme SOLLTE nur von autorisierten Personen (Administratoren oder vertraglich gebundenen Dienstleistern) nach einem definierten Prozess in einer Installationsumgebung durchgeführt werden. Nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTEN die Grundeinstellungen überprüft werden. Sofern die Installation und Konfiguration den Vorgaben aus der Sicherheitsrichtlinie entsprechen, SOLLTEN die Clients im Anschluss in der Produktivumgebung in Betrieb genommen werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass diese durch einen sachkundigen Dritten nachvollzogen und wiederholt werden können.

### SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S)

Nach der Installation SOLLTE überprüft werden, welche Komponenten der Firmware sowie des Betriebssystems und welche Anwendungen und weiteren Tools auf den Clients installiert und aktiviert sind. Nicht benötigte Module, Programme, Dienste, Aufgaben und Firmwarefunktionen (wie Fernwartung) SOLLTEN deaktiviert oder ganz deinstalliert werden. Nicht benötigte Laufzeitumgebungen, Interpretersprachen und Compiler SOLLTEN deinstalliert werden. Nicht benötigte Benutzerkennungen SOLLTEN deaktiviert oder gelöscht werden. Nicht benötigte Schnittstellen und Hardware des IT-Systemes (wie Webcams) SOLLTEN deaktiviert werden. Es SOLLTE verhindert werden, dass diese Komponenten wieder reaktiviert werden können. Die getroffenen Entscheidungen SOLLTEN nachvollziehbar dokumentiert werden.

### SYS.2.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

### SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen (S)

Kommunikationsverbindungen SOLLTEN, soweit möglich, durch Verschlüsselung geschützt werden.

Die Clients SOLLTEN kryptografische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen.

Neue Zertifikate von Zertifikatsaustellern SOLLTEN erst nach Überprüfung des Fingerprints aktiviert werden.

### SYS.2.1.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

### SYS.2.1.A20 Schutz der Administrationsverfahren bei Clients (S)

Abhängig davon, ob Clients lokal oder über das Netz administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Verfahren SOLLTEN über die in der Sicherheitsrichtlinie festgelegten Vorgaben erfolgen.

### SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras (S)

Der Zugriff auf Mikrofon und Kamera eines Clients SOLLTE nur durch den Benutzer selbst möglich sein, solange er lokal am IT-System arbeitet. Wenn vorhandene Mikrofone oder Kameras nicht genutzt und deren Missbrauch verhindert werden soll, SOLLTEN diese, wenn möglich, ausgeschaltet, abgedeckt (nur Kamera), deaktiviert oder physisch vom Gerät getrennt werden. Es SOLLTE geregelt werden, wie

Kameras und Mikrofone in Clients genutzt und wie die Rechte vergeben werden.

**SYS.2.1.A22 ENTFALLEN (S)**
Diese Anforderung ist entfallen.

**SYS.2.1.A23 Bevorzugung von Client-Server-Diensten (S)**
Wenn möglich, SOLLTEN zum Informationsaustausch dedizierte Serverdienste genutzt und direkte Verbindungen zwischen Clients vermieden werden. Falls dies nicht möglich ist, SOLLTE festgelegt werden, welche Client-zu-Client-Dienste (oft auch als „Peer-to-Peer" bezeichnet) genutzt und welche Informationen darüber ausgetauscht werden dürfen. Falls erforderlich, SOLLTEN die Benutzer für die Nutzung solcher Dienste geschult werden. Direkte Verbindungen zwischen Clients SOLLTEN sich nur auf das LAN beschränken. Auto-Discovery-Protokolle SOLLTEN auf das notwendige Maß beschränkt werden.

**SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern (S)**
Auf externe Schnittstellen SOLLTE NUR restriktiv zugegriffen werden können. Es SOLLTE untersagt werden, dass nicht zugelassene Geräte oder Wechseldatenträger mit den Clients verbunden werden. Es SOLLTE verhindert werden, dass von den Clients auf Wechseldatenträger aus nicht vertrauenswürdigen Quellen zugegriffen werden kann. Die unerlaubte Ausführung von Programmen auf bzw. von externen Datenträgern SOLLTE technisch unterbunden werden. Es SOLLTE verhindert werden, dass über Wechsellaufwerke oder externe Schnittstellen unberechtigt Daten von den Clients kopiert werden können.

**SYS.2.1.A25 ENTFALLEN (S)**
Diese Anforderung ist entfallen.

**SYS.2.1.A26 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)**
Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, SOLLTEN ASLR und DEP/NX im Betriebssystem aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken wie z. B. Heap- und Stackschutz SOLLTEN aktiviert werden.

**SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients (S)**
Bei der Außerbetriebnahme eines Clients SOLLTE sichergestellt werden, dass keine Daten verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf den IT-Systemen gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines IT-Systems abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

**SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients (S)**
Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Dafür SOLLTEN Sicherheitsrichtlinien, unter Berücksichtigung der Empfehlungen des Betriebssystemherstellers und des voreingestellten Standardverhaltens, konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem IT-Grundschutz oder der Organisation widerspricht. Die Entscheidungen SOLLTEN dokumentiert und begründet werden. Sicherheitsrichtlinien SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn das voreingestellte Standardverhalten dadurch nicht verändert wird.

**SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients (S)**
Alle Einstellungen der Clients SOLLTEN durch Nutzung eines Managementsystems verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert sein. Konfigurationsänderungen SOLLTEN dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt werden, sodass der Stand der Sicherheitskonfiguration jederzeit nachvollziehbar ist und Konfigurationsänderungen schnell durchgeführt und zentralisiert verteilt werden können.

## 3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.2.1 *Allgemeiner Client* 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.2.1.A28 Verschlüsselung der Clients (H)

Wenn vertrauliche Informationen auf den Clients gespeichert werden, SOLLTEN mindestens die schutzbedürftigen Dateien sowie ausgewählte Dateisystembereiche oder besser die gesamten Datenträger verschlüsselt werden. Hierfür SOLLTE ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden. In diesem Zusammenhang SOLLTEN die Authentisierung (z. B. Passwort, PIN, Token), die Ablage der Wiederherstellungsinformationen, die zu verschlüsselnden Laufwerke und die Schreibrechte auf unverschlüsselte Datenträger geregelt werden. Der Zugriff auf das genutzte Schlüsselmaterial MUSS angemessen geschützt sein.

Benutzer SOLLTEN darüber aufgeklärt werden, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben.

### SYS.2.1.A29 Systemüberwachung und Monitoring der Clients (H)

Die Clients SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden, das den Systemzustand und die Funktionsfähigkeit der Clients laufend überwacht und Fehlerzustände sowie die Über- bzw. Unterschreitung definierter Grenzwerte an das Betriebspersonal meldet.

### SYS.2.1.A30 Einrichten einer Referenzumgebung für Clients (H)

Für Clients SOLLTE eine Referenzinstallation erstellt werden, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Client vorab getestet werden können. Für verschiedene, typische und häufig wiederkehrende Testfälle SOLLTEN Checklisten erstellt werden, die beim Testlauf möglichst automatisiert abgearbeitet werden sollten. Die Testfälle SOLLTEN sowohl die Anwendersicht als auch die Betriebsperspektive berücksichtigen. Zusätzlich SOLLTEN alle Tests so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

### SYS.2.1.A31 Einrichtung lokaler Paketfilter (H)

Auf jedem Client SOLLTEN, zusätzlich zu den eingesetzten zentralen Sicherheitsgateways, lokale Paketfilter eingesetzt werden. Als Strategie zur Paketfilter-Implementierung SOLLTE eine Whitelist-Strategie gewählt werden, die auf Basis der benötigten Netzkommunikation erfolgt.

### SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (H)

Auf den Clients SOLLTEN zusätzliche Maßnahmen zum expliziten Schutz vor Exploits (Angriffe, um Systemlücken auszunutzen) getroffen werden. Wenn notwendige Schutzmaßnahmen nicht über Funktionen des Betriebssystems umgesetzt werden können, SOLLTEN zusätzliche geeignete Sicherheitsmaßnahmen umgesetzt werden. Sollte es nicht möglich sein, nachhaltige Maßnahmen umzusetzen, SOLLTEN andere geeignete (in der Regel organisatorische) Sicherheitsmaßnahmen ergriffen werden.

### SYS.2.1.A33 Application Whitelisting (H)

Es SOLLTE über Application Whitelisting sichergestellt werden, dass nur explizit erlaubte Programme und Skripte ausgeführt werden können. Die Regeln SOLLTEN so eng wie möglich gefasst werden. Falls Pfade und Hashes nicht explizit angegeben werden können, SOLLTEN alternativ auch zertifikatsbasierte oder Pfad-Regeln genutzt werden.

### SYS.2.1.A34 Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (H)

Um sowohl den Zugriff eines Angreifers auf das Betriebssystem oder andere Anwendungen als auch

den Zugriff vom Betriebssystem auf besonders schützenswerte Dateien zu verhindern, SOLLTEN Anwendungen und Betriebssystemkomponenten (wie beispielsweise Authentisierung oder Zertifikatsüberprüfung) besonders gekapselt bzw. anderen Anwendungen und Betriebssystemkomponenten gegenüber isoliert werden. Dabei SOLLTEN insbesondere sicherheitskritische Anwendungen berücksichtigt werden, die mit Daten aus unsicheren Quellen arbeiten (z.B. Webbrowser und Bürokommunikations-Anwendungen).

**SYS.2.1.A35 Aktive Verwaltung der Wurzelzertifikate (H)**

Im Zuge der Beschaffung und Installation des Clients SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Clients notwendig sind. Auf dem Client SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden (z. B. UEFI-Zertifikatsspeicher, Zertifikatsspeicher von Web-Browsern etc.).

**SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM (H)**

Auf UEFI-kompatiblen Systemen SOLLTEN Bootloader, Kernel sowie alle benötigten Firmware-Komponenten durch selbstkontrolliertes Schlüsselmaterial signiert und nicht benötigtes Schlüsselmaterial SOLLTE entfernt werden. Sofern das Trusted Platform Module (TPM) nicht benötigt wird, SOLLTE es deaktiviert werden.

**SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung (H)**

Es SOLLTE eine sichere Mehr-Faktor-Authentisierung unter Einbeziehung unterschiedlicher Faktoren (Wissen, Besitz, Eigenschaft) für die lokale Anmeldung am Client eingerichtet werden, z. B. Passwort mit Chipkarte oder Token.

**SYS.2.1.A38 Einbindung in die Notfallplanung (H)**

Die Clients SOLLTEN im Notfallmanagementprozess berücksichtigt werden. Die Clients SOLLTEN hinsichtlich der Geschäftsprozesse oder Fachaufgaben, für die sie benötigt werden, für den Wiederanlauf priorisiert werden. Es SOLLTEN geeignete Notfallmaßnahmen vorgesehen werden, indem mindestens Wiederanlaufpläne erstellt, Bootmedien zur Systemwiederherstellung generiert sowie Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

**SYS.2.1.A39 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (H)**

Clients SOLLTEN an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV SOLLTE hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Clients SOLLTEN vor Überspannung geschützt werden.

**SYS.2.1.A40 Betriebsdokumentation (H)**

Die Durchführung betrieblicher Aufgaben an Clients bzw. Clientgruppen SOLLTE nachvollziehbar anhand der Fragen „Wer?“, „Wann?“ und „Was?“ dokumentiert werden. Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Auch sicherheitsrelevante Aufgaben (z. B. wer befugt ist, neue Festplatten einzubauen) SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE vor unbefugtem Zugriff und Verlust geschützt werden. Sicherheitsrelevante Aspekte SOLLTEN nachvollziehbar erläutert und hervorgehoben werden.

**SYS.2.1.A41 Verwendung von Quotas für lokale Datenträger (H)**

Es SOLLTE überlegt werden, Quotas einzurichten, die den verwendeten Speicherplatz auf der lokalen Festplatte begrenzen. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystems genutzt werden, die den Benutzer bei einem bestimmten Füllstand der Festplatte warnen oder nur noch dem Systemadministrator Schreibrechte einräumen.

**SYS.2.1.A45 Erweiterte Protokollierung (H)**

Es SOLLTE auch Client-Verhalten, das nicht mit der Sicherheit direkt in Verbindung steht, protokolliert

und unverzüglich (automatisiert) ausgewertet werden, um verdeckte Angreiferaktivitäten erkennen zu können.

# 4 Weiterführende Informationen

## 4.1 Wissenswertes

Für den Baustein SYS.2.1 *Allgemeiner Client* sind keine weiterführende 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.2.1 *Allgemeiner Client* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen