|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Clients unter macOS"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300031 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Clients unter macOS" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc80728719)

[Dokumentenhistorie 3](#_Toc80728720)

[Inhaltsverzeichnis 4](#_Toc80728721)

[Allgemeine Festlegungen 5](#_Toc80728722)

[Ziel / Zweck 5](#_Toc80728723)

[Geltungsbereich 5](#_Toc80728724)

[Zuständigkeiten 6](#_Toc80728725)

[Genehmigungs- und Änderungsverfahren 6](#_Toc80728726)

[Aufbau des Dokuments 6](#_Toc80728727)

[Sicherheitsrichtlinie „Clients unter macOS" 7](#_Toc80728728)

[Basismaßnahmen 7](#_Toc80728729)

[Allgemeiner Client 7](#_Toc80728730)

[Clients unter macOS 9](#_Toc80728731)

[Standardmaßnahmen 9](#_Toc80728732)

[Allgemeiner Client 10](#_Toc80728733)

[Clients unter macOS 13](#_Toc80728734)

[Maßnahmen bei erhöhtem Schutzbedarf 15](#_Toc80728735)

[Allgemeiner Client 15](#_Toc80728736)

[Clients unter macOS 17](#_Toc80728737)

# Allgemeine Festlegungen

## Ziel / Zweck

macOS ist ein Client-Betriebssystem der Firma Apple. macOS selbst basiert auf Darwin, dem frei verfügbaren Unix-Betriebssystem der Firma Apple, das wiederum auf dem Open-Source-Betriebssystem FreeBSD aufbaut. macOS setzt sich im Wesentlichen aus Darwin sowie der proprietären grafischen Bedienoberfläche „Aqua“ und weiteren Anwendungen und Diensten zusammen. Gemäß den Lizenzbedingungen von Apple darf macOS nur auf IT-Systemen („Macs“) von Apple installiert werden. Aus diesem Grund sind Eigenheiten dieser Systeme ebenfalls Bestandteil dieser Sicherheitsrichtlinie. Zusätzlich zu den macOS spezifischen Anforderungen an die Absicherung sind generelle Absicherungen („Allgemeiner Client“), welche für alle Client Betriebssysteme anwendbar innerhalb der <Institution> zu etablieren

Als „Allgemeiner Client“ wird ein Client-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. Typischerweise ist ein solches IT-System vernetzt und in ein Client-Server-Netz bzw. Client-Cloud-Infrastruktur-Netz eingebunden. Das IT-System verfügt in der Regel über Laufwerke für auswechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte.

Das Ziel dieser Sicherheitsrichtlinie ist der Schutz von Informationen, die auf IT-Systemen unter macOS verarbeitet oder mit diesen übertragen werden. Die Sicherheitsrichtlinie zielt außerdem darauf ab, Geschäftsprozesse und andere IT-Systeme davor zu schützen, durch Macs beeinträchtigt zu werden. Dazu müssen IT-Systeme unter macOS angemessen abgesichert werden. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine SYS.2.1 "Allgemeiner Client" und SYS.2.4 "Clients unter macOS" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Clients unter macOS“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Clients unter macOS"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Allgemeiner Client

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

Um den Client zu nutzen sind die Mitarbeitenden gegenüber dem IT-System zu authentisieren. Sollen die Mitarbeitenden hierfür Passwörter verwenden, müssen sichere Passwörter gewählt werden. Die verwendeten Passwörter müssen den Vorgaben der <Institution> entsprechen.

#### Rollentrennung (SYS.2.1.A2)

Der Client ist so einzurichten, dass normale (tägliche) Tätigkeiten nicht mit Administratorrechten ausgeübt werden. Nur Mitarbeitende der Gruppe Administratoren dürfen Administratorrechte erhalten. Die Installation, Modifikation, Änderung oder Löschung von Anwendungen und Systemkonfigurationen darf nur durch die Administration unter Zuhilfenahme von zentralen Managementwerkzeugen erfolgen. Mitarbeitende dürfen nur ausschließlich lesenden Zugriff auf Systemdateien haben.

Ablauf, Rahmenbedingungen und Anforderungen an administrative Aufgaben sowie die Aufgabentrennungen zwischen den verschiedenen Rollen der Mitarbeitenden (Benutzer) des IT-Systems sollten in einem Benutzer- und Administrationskonzept festgeschrieben werden.

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

Um zu verhindern, dass Attacker die identifizierten Schwachstellen des Client-Betriebssystem ausnutzen, sind automatische Update-Mechanismen (Autoupdate) zu etablieren. Sofern andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden, kann auf automatische Update-Mechanismen verzichtet werden. Hierbei ist jedoch sicherzustellen, dass die neuesten Sicherheitsupdates zeitnah nach Veröffentlichung installiert werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, sollte mindestens täglich automatisch nach Updates gesucht und die Updates installiert werden.

#### Regelmäßige Datensicherung (SYS.2.1.A4)

Die Clients sind in ein Datensicherungskonzept der <Institution> einzubeziehen. Es sind Regelungen zu definieren, welche lokal auf dem Client abgespeicherten Daten wie, von wem, wann und wie regelmäßig gesichert werden. Es sind mindestens diejenigen Daten regelmäßig zu sichern, die nicht aus anderen Informationen abgeleitet werden können. Bei vertraulichen und ausgelagerten Backups sind die gesicherten Daten verschlüsselt zu speichern. Für eingesetzte Anwendungssoftware sollte separat entschieden werden, ob die Software von der regelmäßigen Datensicherung erfasst werden muss. Die Mitarbeitenden sollten über die Regelungen zur Datensicherung informiert werden.

Es ist regelmäßig zu verifizieren, ob die etablierte Datensicherung wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können.

#### Verwendung einer Bildschirmsperre (SYS.2.1.A5)

Damit Unbefugte nicht auf aktive Clients zugreifen können, ist eine Bildschirmsperre zu verwenden. Die Bildschirmsperre sollte sich sowohl manuell vom Mitarbeitenden aktivieren lassen als auch nach 15 Minuten der Client Inaktivität automatisch gestartet werden. Es ist sicherzustellen, dass die Bildschirmsperre erst nach einer erfolgreichen Authentisierung des Mitarbeitenden am Client deaktiviert wird.

#### Einsatz von Viren-Schutzprogrammen (SYS.2.1.A6)

Abhängig vom installierten Betriebssystem und anderen vorhandenen Schutzmechanismen ist auf allen Clients der <Institution> eine Antivirenlösung zu installieren und zu aktivieren. Es muss sichergestellt sein, dass sowohl das Scan-Programm als auch die Signaturen stets auf dem aktuellen Stand sind. Die Mitarbeitenden sind über den Umgang mit der Antivirenlösung und On-Demand-Scans zu unterrichten. Die Antivirenlösung auf den Clients ist so zu konfigurieren, dass die Mitarbeitenden weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen können und die Antivirenlösung nicht deaktivieren können.

Der gesamte Datenbestand der Clients ist regelmäßig auf Schadprogramme zu prüfen. Wenn das Laptop infiziert ist, ist im Offlinebetrieb zu untersuchen, ob das gefundene Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen wurde. Da eine Offline Untersuchung nur möglich ist, wenn zuvor alle sich im Laptop befindlichen Datenspeicher entschlüsselt wurden, ist eine Cloud-basierte Antivirenlösungen der nächsten Generation mit erweiterter Endpoint-Detection and Response (EDR) zu etablieren.

Die Antivirenlösung muss zudem nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Auch müssen alle auf dem Laptop benutzten Internet-Dienste (HTTP, FTP) sowie verschlüsselte Daten ausreichend vor Schadprogrammen geschützt werden.

#### Protokollierung auf Clients (SYS.2.1.A7)

Es ist zu definieren, welche Informationen auf Clients mindestens protokolliert werden sollen, wie lange die Protokolldaten aufbewahrt werden und wer unter welchen Voraussetzungen die Protokolldaten einsehen darf. Generell sind alle sicherheitsrelevanten Systemereignisse zu protokollieren. Es sollte geprüft werden, ob die Speicherung der Protokolldaten auf den jeweiligen Clients selbst ausreichend ist oder ob eine zentrale Speicherung erfolgen muss.

Unabhängig, ob sich für eine lokale oder zentrale Protokollierung entschieden wird, ist in geeigneten Intervallen Stichpunkt-artig zu überprüfen, ob die Protokollierung noch korrekt funktioniert. Die Intervalle sind an die betrachteten Zielobjekte und den Schutzbedarf der Informationen der vom Client verarbeiteten Daten anzupassen.

Bei der Protokollierung werden die gesetzlichen Bestimmungen aus den aktuellen Gesetzen zum Datenschutz eingehalten. Dazu zählen unter anderem die gesetzlichen Anforderungen der EU-DSGVO und des BDSG-neu. Darüber hinaus sind eventuelle Persönlichkeitsrechte zu wahren. Es ist sicherzustellen, dass alle weiteren relevanten gesetzlichen Bestimmungen und die Anforderungen der Kunden beachtet werden.

Die Protokollierungsdaten sind nach einem festgelegten Aufbewahrungsprozess zu löschen. Es ist technisch zu unterbinden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden können.

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

Der Startvorgang des Clients („Booten“) muss gegen Manipulation abgesichert werden. Es ist festzulegen, von welchen Medien gebootet werden darf. Es sollte entschieden werden, ob und wie der Bootvorgang kryptografisch geschützt werden soll. Es ist sicherzustellen, dass nur Mitarbeitende der Gruppe "Administratoren" die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können. Nur Mitarbeitende der Gruppe "Administratoren" dürfen von eventuell eingebauten optischen oder vorhandenen externen Speichermedien booten können. Die Konfigurationseinstellungen des Bootvorgangs dürfen nur durch Mitarbeitende der Gruppe "Administratoren" verändert werden können. Alle nicht benötigten Funktionen sind in der Firmware (UEFI/BIOS) zu deaktivieren.

### Clients unter macOS

#### Planung des sicheren Einsatzes von macOS (SYS.2.4.A1)

Die Einführung von macOS-Clients muss seitens der <Institution> sorgfältig geplant werden. Im Rahmen der Planung sind ein Konzept zur Geräteverwaltung, Benutzerverwaltung, zur Administration, zum Patchen und zur Aktualisierung von Software, zum Schutz vor Schadsoftware, zur Datensicherung sowie zur Protokollierung zu erstellen und deren Integration in bestehende Konzepte auf zu zeigen. Ebenfalls Bestandteil der Planung ist die Definition, wo und wie Daten der macOS-Clients und Mitarbeitenden abgelegt werden.

Sofern ein Plattformwechsel zu macOS geplant ist, muss ein Migrationskonzept erstellt werden.

#### Nutzung der integrierten Sicherheitsfunktionen von macOS (SYS.2.14A2)

Die in macOS integrierten Schutzmechanismen „System Integrity Protection“ (SIP), „Xprotect“ und „Gatekeeper“ müssen aktiviert sein und dürfen nicht durch die Gruppe der Administratoren deaktiviert werden. Die Einstellungen des Gatekeepers dürfen nur die Ausführung von signierten Anwendungen erlauben. In begründeten Ausnahmen dürfen nach Abstimmung mit dem <Datenschutzbeauftragter> und dem <Informationssicherheitsbeauftragter> unsignierte Anwendungen in den Softwarebereitstellungsprozess aufgenommen werden.

#### Verwendung geeigneter Benutzerkonten (SYS.2.4.A3)

Das bei der Erstkonfiguration von macOS angelegte Administrator-Konto darf nur zu administrativen Zwecken verwendet werden. Für die normale Verwendung des macOS-Clients ist zusätzlich ein Standard-Benutzerkonto anzulegen. Sollte der macOS-Client von mehreren Mitarbeitenden verwendet werden, ist für jeden Mitarbeitenden ein eigenes personalisiertes Benutzerkonto anzulegen werden. Das Gast-Benutzerkonto muss deaktiviert werden.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Allgemeiner Client

#### Planung des Einsatzes von Clients (SYS.2.1A10)

Damit Clients sicher betrieben werden können, sollte im Vorfeld geplant werden, wo und wie diese eingesetzt werden sollen. Die Planung sollte dabei nicht nur Aspekte betreffen, die typischerweise mit dem Begriff „Sicherheit“ verknüpft werden, sondern auch normale betriebliche und Aspekte zur Benutzerfreundlichkeit die Anforderungen im Bereich der Sicherheit nach sich ziehen. Neben Client-Typ-spezifischen Anforderungsprofilen sind Vorgaben zur Authentisierung und Benutzerverwaltung zu definieren. Alle Entscheidungen, die in der Planungsphase getroffen wurden, sollten so dokumentiert werden, dass die Entscheidungen zu einem späteren Zeitpunkt nachvollzogen werden können.

#### Beschaffung von Clients (SYS.2.1.A11)

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 müssen für den gesamten geplanten Nutzungszeitraum Patches für Schwachstellen zeitnah zur Verfügung stellen. Die zu beschaffenden Systeme müssen über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot verfügen. Sofern vorhanden solle der Client auch über ein TPM verfügen.

#### Kompatibilitätsprüfung von Software (SYS.2.1.A12)

Bevor zusätzliche Software für die Clients beschafft wird, ist zu prüfen, ob die Software mit dem eingesetzten Betriebssystem in der vorliegenden Konfiguration kompatibel ist. Die Kompatibilitätsprüfung muss in das Freigabeverfahren der Software aufgenommen werden. Gibt es vom Softwarehersteller oder aus anderen Fachkreisen keine verbindliche Information zur Kompatibilität, sollte die Kompatibilität in einer Testumgebung oder im Rahmen eines Proof-of-Concepts geprüft werden. Vor einer beabsichtigten Hardwareänderung oder bei einer Betriebssystemmigration muss die Kompatibilität der Treibersoftware für alle betroffenen Komponenten gewährleistet werden.

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

Der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (z. B. durch das Betriebssystem speziell abgesicherte Speicherbereiche, Firmwarebereiche oder die Nutzung von sudo) darf nur durch Mitarbeitende mit administrativen Berechtigungen möglich sein. Die entsprechenden Einstellungen in der BIOS/UEFI-Firmware sollte durch ein Passwort vor unberechtigten Veränderungen geschützt werden. Wird die Kontrolle über die Funktionen an das Betriebssystem delegiert, dürfen auch dort nur Mitarbeitende mit administrativen Berechtigungen auf die Funktionen zugreifen dürfen.

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

Die Verantwortlichen Administratoren müssen sich regelmäßig über bekannt gewordene Schwachstellen in Firmware, Betriebssystemen und Anwendungen der betreuten Clients informieren. Die identifizierten Schwachstellen sind zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität zu beheben bzw. falls erforderlich ein Workaround bis zur finalen Behebung zu etablieren. Generell ist darauf zu achten, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden. Falls notwendig, sollten die betreffenden Anwendungen beziehungsweise das Betriebssystem nach dem Update neu gestartet werden.

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

Es sollte festgelegt werden, welche Komponenten des Betriebssystems, welche Anwendungen und welche weiteren Tools installiert werden sollen. Die Installation und Konfiguration der Clients sollten nur von autorisierten Mitarbeitenden bzw. vertraglich gebundenen Dienstleistern nach einem definierten Prozess durchgeführt werden. Alle Installations- und Konfigurationsschritte sollten so dokumentiert werden, dass die Installation und Konfiguration durch einen sachkundigen Dritten anhand der Dokumentation nachvollzogen und wiederholt werden kann (siehe Anforderung "Betriebsdokumentation/Betriebshandbuch").

Die Factory-Default Einstellungen von Clients sind zu überprüfen und bei Bedarf entsprechend den internen Vorgaben der <Institution> anzupassen. Erst nachdem die Installation und die Konfiguration abgeschlossen sind, sollte der Client mit dem produktiven Netz bzw. dem Internet direkt verbunden werden.

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

Nach der Installation ist zu überprüfen, 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, Benutzerkennungen und Schnittstellen sind zur Reduzierung des Angriffsvektors zu deaktivieren oder ganz zu entfernen. Außerdem sollten nicht benötigte Laufzeitumgebungen, Interpreter Sprachen und Compiler deinstalliert werden. Entsprechende nicht benötigte, jedoch fest mit dem IT-System verbundene Komponenten sollten sofern möglich deaktiviert werden. Auch in der Firmware vorhandene und nicht benötigte Komponenten (z. B. Fernwartung) sollten sofern es der Schutzbedarf des Clients erfordert abgeschaltet werden. Es ist zu verhindern, dass die deaktivierten Komponenten unberechtigt wieder reaktiviert werden können. Die getroffenen Entscheidungen, welche Komponenten zu deaktivieren bzw. zu entfernen sind, sollte nachvollziehbar dokumentiert werden.

#### Einsatzfreigabe für Clients (SYS.2.1.A17)

Bevor der Client im produktiven Betrieb eingesetzt und bevor der Client an die produktiven Netze der <Institution> angeschlossen wird, sollte eine Einsatzfreigabe erfolgen. Die Einsatzfreigabe sollte nachvollziehbar dokumentiert werden. Für die Einsatzfreigabe sollte die Installations- und Konfigurationsdokumentation und die Funktionsfähigkeit der Clients in einem Test geprüft werden.

#### Nutzung von TLS (SYS.2.1.A18)

Zur Erhöhung des Sicherheitsniveaus sollten Kommunikationsverbindungen ausgehend vom Client kryptographisch abgesichert werden und nur die freigebenden Protokolle und deren Algorithmen und Schlüssellängen unterstützen. Mitarbeitende sollten zusätzlich darauf achten, dass die besuchten Webseiten nur eine verschlüsselte Verbindung mittels Transport Layer Security (TLS) anbieten. Dies ist erkennbar an dem geschlossenen Schloss-Symbol.

Die Verantwortlichen Administratoren sollte durch zentrale Konfigurationsvorgaben dafür sorgen, dass die freigegebenen Clients nur die bei der <Institution> freigegebenen sicheren Version von TLS unterstützen.

Neue Zertifikate sollten erst nach Überprüfung des „Fingerprints“ aktiviert werden. Die Überprüfung von Zertifikaten sollte in Anwendungsprogrammen wie Browsern und E-Mail-Clients aktiviert werden. Session Renegotiation und TLS-Kompression sollten hingegen deaktiviert werden.

#### Restriktive Rechtevergabe (SYS.2.1.A19)

Der verfügbare Funktionsumfang der Clients sollte für einzelne Mitarbeitende oder Gruppen so eingeschränkt werden, so das nur die wirklich benötigten Rechte und Funktionen für ihre Aufgabenwahrnehmung bereitgestellt werden („Need-to-know-Prinzip“). Zugriffsberechtigungen sollten hierfür möglichst restriktiv vergeben werden. Es sollte regelmäßig überprüft werden, ob die vergebenen Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben des Need-to-know-Prinzips entsprechen. Auf Systemdateien des Clients dürfen nur die Mitarbeitenden der Rolle "Systemadministratoren" zugreifen können. Der Gruppe der zugriffsberechtigten Systemadministratoren ist möglichst klein zu halten.

#### Schutz der Administrationsschnittstellen (SYS.2.1.A20)

In Abhängigkeit, ob Clients lokal oder zentral administriert werden, sollten geeignete Sicherheitsvorkehrungen zur Absicherung der Administrationsschnittstellen getroffen werden. Die zur Administration verwendeten Methoden sollten zuvor festgelegt und etabliert werden. Erfolgt die Administration der Clients über das Netz der <Institution> oder über öffentliche Netze müssen hierfür freigegebene sichere Protokolle verwendet werden.

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

Der Zugriff auf Mikrofon und Kamera eines Clients sollte nur den vom Mitarbeitenden aktuell genutzten Anwendungen möglich sein. Wenn vorhandene Mikrofone oder Kameras nicht genutzt oder deren Missbrauch proaktiv verhindert werden soll, sollte die Kamera abgedeckt oder deaktiviert bzw. die Aktivierung der Kamera oder des Mikrofons im Hintergrund automatisch überwacht werden.

Sofern keine Tool-Unterstützung zur Überwachung der Client-Kamera und des Client-Mikrofones etabliert wird, ist mindestens die Kamera bei Nichtgebrauch abzudecken.

#### Abmelden nach Aufgabenerfüllung (SYS.2.1.A22)

Es sind alle Mitarbeitende zu verpflichten, sich nach Aufgabenerfüllung (Feierabend) vom Client bzw. vom Betriebssystem abzumelden. Ist für einen Mitarbeitenden absehbar, dass die Arbeit nur kurz unterbrochen wird, sollte die Bildschirmsperre manuell durch den Mitarbeitenden aktiviert werden, statt sich vom Client abzumelden.

#### Bevorzugung von Client-Server-Diensten (SYS.2.1.A23)

Wenn möglich, sollten zum Informationsaustausch dedizierte Serverdienste oder von der <Institution> freigegeben Cloud-Dienste/WebApp's genutzt werden. Direkte Verbindungen zwischen Clients sind zu vermeiden. Sollte dies nicht möglich sein, dürfen nur zuvor freigegebene Client-zu-Client-Dienste („Peer-to-Peer“) genutzt werden. Falls erforderlich, sollten die Mitarbeitenden für die Nutzung von Client-zu-Client-Diensten geschult werden. Grundsätzlich gilt, direkte Verbindungen zwischen Clients sind auf das produktive LAN der <Institution> zu beschränken.

Auto-Discovery-Protokolle sollten auf das notwendige Maß beschränkt werden.

#### Umgang mit externen Medien und Wechseldatenträgern (SYS.2.1.A24)

Es sollte verhindert werden, dass über Wechsellaufwerke oder externe Schnittstellen unkontrolliert Software auf den Clients installiert werden kann oder unberechtigt Daten von den Clients kopiert werden können. Auf externe Schnittstellen sollte nur restriktiv zugegriffen werden können. Es sollte grundsätzlich verhindert werden, dass von den Clients auf Daten oder Wechseldatenträger aus nicht vertrauenswürdigen Quellen zugegriffen wird.

Die Anforderungen an den Umgang mit Wechseldatenträgern sind in der korrespondierenden Sicherheitsrichtlinie beschrieben.

#### Mitarbeiterrichtlinie zur sicheren IT-Nutzung (SYS.2.1.A25)

Die internen Standards der Ebenen 2 des Security-Management-Frameworks beschreiben für alle Mitarbeitenden transparent, welche Rahmenbedingungen bei der IT-Nutzung eingehalten werden müssen und welche Sicherheitsmaßnahmen zu ergreifen sind.

#### Schutz vor Ausnutzung von Schwachstellen in Anwendungen (SYS.2.1.A26)

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, sind ASLR und DEP/NX im Betriebssystem zu aktivieren und von den Anwendungen zu nutzen. Sicherheitsfunktionen des Kernels und der Standardbibliotheken wie z. B. Heap- und Stackschutz dürfen nicht deaktiviert werden.

#### Geregelte Außerbetriebnahme eines Clients (SYS.2.1.A27)

Bei der Außerbetriebnahme eines Clients ist sicherzustellen, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es sollte einen Überblick darüber geben, welche Daten wo auf den IT-Systemen gespeichert sind. Es ist eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Clients abgearbeitet werden sollte. Diese Checkliste umfasst mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten.

### Clients unter macOS

#### Integration von Online-Konten in das Betriebssystem (SYS.2.4.bd.A1)

Die Anmeldung am macOS-Client sollte auf Basis eines zentral verwalteten Verzeichnisdienst erfolgen und sollte ebenfalls zentral verwaltete Apps-IDs einschließen.

#### Verwendung einer Festplattenverschlüsselung (SYS.2.4.A4)

Die Festplatten der macOS-Clients sind entsprechend den freigegebenen Protokollen und Algorithmen zu verschlüsseln. Wird dazu die in macOS integrierte Funktion FileVault verwendet, darf das Schlüsselmaterial nicht online bei der Firma Apple gespeichert werden.

Der von FileVault erzeugte Wiederherstellungsschlüssel ist an einem sicheren Ort aufzubewahren. Es muss geprüft werden, ob ein institutioneller Wiederherstellungsschlüssel (IRK) für FileVault bevorzugt zum Einsatz kommen soll.

#### Deaktivierung sicherheitskritischer Funktionen von macOS (SYS.2.4.A5)

Die im macOS-Client integrierten Ortungsdienste sind sofern es der Schutzbedarf der verarbeiteten Informationen erfordert zu deaktivieren. Heruntergeladene Daten und Inhalte von optischen und anderen Medien dürfen nicht automatisch geöffnet und ausgeführt werden.

#### Verwendung aktueller macOS-Hardware (SYS.2.4.A6)

Werden neue macOS-Client beschafft, sollten aktuelle Modelle ausgewählt werden. Werden bereits macOS-Clients eingesetzt, muss regelmäßig überprüft werden, ob die Clients weiterhin von Apple mit Sicherheits-Updates versorgt werden. Sofern macOS-Clients nicht mehr durch Apple (siehe Link <https://support.apple.com/en-us/HT201624>) unterstützt werden, dürfen diese nicht mehr im produktiven Einsatz weiterverwendet werden.

#### Zwei-Faktor-Authentisierung für Apple-ID (SYS.2.4.A7)

Für die von der <Institution> zur Verfügung gestellten verwalteten Apple-IDs ist die Zwei-Faktor-Authentisierung zu aktivieren.

#### Keine Nutzung von iCloud für schützenswerte Daten (SYS.2.4.A8)

Seitens der <Institution> sollte verhindert werden, dass schützenswerte Daten zwischen mehreren Clients über die iCloud-Dienste synchronisiert werden. Stattdessen sollten Daten nur über von der <Institution> selbst betriebene Dienste synchronisiert werden. Schützenswerte Daten sollten nicht in iCloud gespeichert werden. E-Mails oder Dokumenten, sollten nicht automatisch und unverschlüsselt in iCloud gespeichert werden.

#### Verwendung von zusätzlichen Schutzprogrammen unter macOS (SYS.2.4.A9)

Bei Bedarf, etwa wenn ein Macs in einem heterogenen Netz betrieben wird, SOLLTEN neben den integrierten Schutzmechanismen von macOS zusätzlich Virenschutz-Lösungen von Drittanbietern eingesetzt werden.

#### Aktivierung der Personal Firewall unter macOS (SYS.2.4.A10)

Die Sicherheitsstrategie zur Nutzung der lokalen Firewall von macOS-Clients ist gemäß den Anforderungen an die Firewall-Infrastruktur der <Institution> zu integrieren und umzusetzen. Sofern der Einsatzzweck der macOS-Clients eine hohe Mobilität beinhaltet ist die im macOS-Client integrierte Personal Firewall zu aktivieren und muss mindestens so konfiguriert sein, dass unautorisierte Anwendungen und Dienste daran gehindert werden eingehen Verbindungen zu akzeptieren.

#### Geräteaussonderung von Macs (SYS.2.4.A11)

Bei einer Aussonderung des macOS-Client ist zusätzlich zu den etablierten Off-Boarding-Standards der nichtflüchtige Datenspeicher (NVRAM) zurückzusetzen.

#### Verwendung des Fingerabdrucksensors (SYS.2.4.bd.A1)

Sofern gleichzeitig organisatorisch und technisch geregelt wird, dass die Mitarbeitenden komplexe Passwörter verwenden. Sollte bei macOS-Clients mit biometrischem Fingerabdrucksensor (Touch ID) das Entsperren des macOS-Clients mittels Touch ID den Mitarbeitenden freigegeben werden. Einhergehend mit der Aktivierung der Touch ID sollten Sensibilisierungen der Mitarbeitenden hinsichtlich der Fälschbarkeit von Fingerabdrücken durchgeführt werden.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Allgemeiner Client

#### Verschlüsselung der Clients (SYS.2.1.A28 - CI)

Wenn vertrauliche Informationen auf den Clients gespeichert werden, sind mindestens die schutzbedürftigen Dateien sowie ausgewählte Dateisystembereiche oder besser die gesamte Festplatte basierend auf den freigegebenen Protokollen zu verschlüsselt. 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, Schlüssel), die Ablage der Wiederherstellungsinformationen, die zu verschlüsselnden Laufwerke, die Schreibrechte auf unverschlüsselte Datenträger und die Art und Weise, wie sichergestellt wird, dass die Wiederherstellungsinformationen nur berechtigten Personen zugänglich sind, geregelt werden. Auch verschlüsselte Dateien, Partitionen oder Datenträger sollten regelmäßig gesichert werden, ohne den Nutzen der Verschlüsselung zu untergraben. Das verwendete Schlüsselmaterial darf nicht im Klartext auf den Clients gespeichert werden.

Die Mitarbeitenden sollten darüber aufgeklärt werden, wie sich bei Verlust eines Authentisierungsmittels zu verhalten ist.

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

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 Überschreitung definierter Grenzwerte an die Verantwortlichen für den Betrieb bzw. den vertraglich gebundenen Dienstleister meldet.

#### Einrichten einer Referenzinstallation für Clients (SYS.2.1.A30 - CIA)

Für die freigegebenen Clients sollte eine Referenzinstallation erstellt werden, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den produktiven Clients vorab getestet werden können. Darüber hinaus sollten die Clients mittels Referenzinstallation aufgesetzt werden. Hierzu wird eine funktionierende und auf den Einsatz passende Grundkonfiguration verwendet. Die verwendete Referenzinstallation sollte dokumentiert sein.

Für verschiedene, typische und häufig wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testlauf abgearbeitet werden können. Zusätzlich sollten alle Tests so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

#### Einrichtung lokaler Paketfilter (SYS.2.1.A31 - CA)

Auf den Clients sollten, zusätzlich zu den eingesetzten zentralen Firewalls, lokale Paketfilter eingesetzt werden. Als Strategie zur Implementierung der Filterregel sollte der Whitelist-Ansatz etabliert werden.

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

Es sollten auf den Clients Tools eingesetzt werden, die im Rahmen eines exploit-basierten Angriffs die Ausnutzung von Software-Sicherheitslücken erkennen und unterbinden. Mithilfe dieser Tools und deren Wirkungsweise können auch für einen zuvor festgelegten Zeitraum nicht gepatchte oder nicht mehr unterstützte Clients sowie nicht registrierte Anwendungen geschützt werden.

Bei der Evaluierung des Tools müssen mindestens die folgenden Kriterien erfüllt sein:

* Der Präventivschutz verhindert die Schwachstellensuche mithilfe von Exploit-Kits.
* Die methodenbasierte Angriffsabwehr schützt vor bekannten Bedrohungen, Zero-Day-Exploits und nicht gepatchten Sicherheitslücken.
* Der Schutz vor Kernel-Exploits sichert das Betriebssystem davor die Sicherheitslücken im Kernel ausnutzen und Prozesse mit ausgeweiteten Berechtigungen (auf Systemebene) zu erstellen/starten.

#### Application Whitelisting (SYS.2.1.A33 - CIA)

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

#### Einsatz von Anwendungsisolation (SYS.2.1.A34 -CI)

Anwendungen, mit denen externe Daten bzw. Daten aus unsicheren Quellen bearbeitet werden, sollten ausschließlich in einer vom Betriebssystem isolierten Ablaufumgebung (Sandbox) betrieben werden.

#### Aktive Verwaltung der Wurzelzertifikate (SYS.2.1.A35 - CI)

Auf dem Client sollten lediglich die für den Betrieb notwendigen und gültigen Wurzelzertifikate (root Zertifikate) der vertrauenswürdigen Zertifizierungsstellen enthalten sein. Es sollte regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der <Institution> entsprechen. Im Rahmen der Überprüfung, sollten auch vorhandene Zertifikatsspeicher wie den UEFI-Zertifikatsspeicher sowie vom Web-Browsern inkludiert sein.

#### Selbstverwalteter Einsatz von SecureBoot und TPM (SYS.2.1.A36 - CI)

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

#### Verwendung von Mehr-Faktor-Authentisierung (SYS.2.1.A37 - CI)

Sind durch die Verarbeitung von Informationen mit hohem Schutzbedarf erhöhte Absicherungen eines Clients notwendig, ist der Zugang zum Client durch die Verwendung einer Mehrfaktorauthentisierung zu schützen.

#### Einbindung in die Notfallplanung (SYS.2.1.A38 - CIA)

Die Clients sind im Notfallmanagementprozess zu berücksichtigen. Die Clients sollten hinsichtlich der Geschäftsprozesse oder Fachaufgaben, für die Clients benötigt werden beim Wiederanlauf bzw. der Wiederherstellung priorisiert werden. Es sollten geeignete Notfallmaßnahmen im Rahmen der Erstellung von Wiederanlauf und Wiederherstellungsplänen sowie idealerweise von Wiederanlaufkoordinationsplänen vorgesehen werden.

#### Unterbrechungsfreie und stabile Stromversorgung (SYS.2.1.A39 - A)

Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients (Workstations) sollten diese an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Wenn Änderungen an den Verbrauchern der USV durchgeführt wurden, sollte erneut geprüft werden, ob die Stützzeit ausreichend ist. Sowohl für die USV-Geräte als auch die Clients sollte ein Überspannungsschutz vorhanden sein.

Die tatsächliche Kapazität der Batterie der USV-Geräte und damit die Stützzeit der USV selbst ist regelmäßig zu testen und zu warten.

#### Betriebsdokumentation (SYS.2.1.A40 - A)

Die Inhalte der Betriebsdokumentation müssen nachvollziehbar sein. Die Betriebsdokumentation sollte angelehnt an den Lebenszyklus folgende inhaltlichen Phasen beinhalten:

* Inbetriebnahme,
* Betrieb,
* Aussonderung und
* Wiederanlauf.

Die Dokumentation muss gegen unbefugten Zugriff geschützt werden. Änderungen müssen nachvollziehbar dokumentiert bzw. referenziert sein.

#### Verhinderung der Überlastung der lokalen Festplatte (SYS.2.1.A41 - CIA)

Sollten der Client hinsichtlich der Geschäftsprozesse oder Fachaufgaben hohe Anforderungen an die Verfügbarkeit erfüllen müssen, sollten Quotas eingerichtet werden. Sofern keine Qutoas eingerichtet werden, kann alternativ auf Mechanismen des verwendeten Datei- oder Betriebssystemsystems zurückgegriffen werden, die den Benutzer bei einem bestimmten Füllstand der Festplatte warnen oder nur noch dem Systemadministrator Schreibrechte einräumen.

### Clients unter macOS

#### Firmware-Kennwort und Boot-Schutz auf Macs (SYS.2.4.A12 - CI)

Um ein unberechtigtes Booten des macOS-Clients von einem anderen Startlaufwerk zu verhindern, sollte die Abfrage eines sicheren Firmware-Kennworts im sogenannten „Command-Modus“ bei macOS-Clients ohne T2-Sicherheitsschip aktiviert werden. Sofern macOS-Clients der <Institution> Informationen mit sehr hohen Schutzbedarf an die Vertraulichkeit und Integrität verarbeiten ist zu prüfen werden, ob über den „Full-Modus“ ein Kennwort bei jedem Startvorgang abgefragt werden sollte.

Auf macOS-Clients mit T2-Sicherheitschip sollte ein Firmware-Passwort über das Startsicherheitsdienstprogramm gesetzt werden. Die Option „Sicheres Starten: Volle Sicherheit“ ist zu aktivieren. Die Option „Starten von externen Medien nicht zulassen“ ist zu aktivieren.

Insofern Systeme mit einer Apple-eigen entwickelten CPU eingesetzt werden, kann diese Anforderungen nicht umgesetzt werden. Zur Mitigation ist es unbedingt erforderlich die Festplattenverschlüsselung zu aktivieren und die Umsetzung von sicheren Passwörtern und 2FA zu achten.