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

Sicherheitsrichtlinie "Windows-Clients"

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 Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300029 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [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](#_Toc80643731)

[Dokumentenhistorie 3](#_Toc80643732)

[Inhaltsverzeichnis 4](#_Toc80643733)

[Allgemeine Festlegungen 5](#_Toc80643734)

[Ziel / Zweck 5](#_Toc80643735)

[Geltungsbereich 5](#_Toc80643736)

[Zuständigkeiten 6](#_Toc80643737)

[Genehmigungs- und Änderungsverfahren 6](#_Toc80643738)

[Aufbau des Dokuments 6](#_Toc80643739)

[Sicherheitsrichtlinie „Windows-Clients" 7](#_Toc80643740)

[Basismaßnahmen 7](#_Toc80643741)

[Allgemeiner Client 7](#_Toc80643742)

[Client unter Windows 10 9](#_Toc80643743)

[Standardmaßnahmen 10](#_Toc80643744)

[Allgemeiner Client 10](#_Toc80643745)

[Client unter Windows 10 14](#_Toc80643746)

[Maßnahmen bei erhöhtem Schutzbedarf 17](#_Toc80643747)

[Allgemeiner Client 17](#_Toc80643748)

[Client unter Windows 10 20](#_Toc80643749)

# Allgemeine Festlegungen

## Ziel / Zweck

Mit Windows 10 hat Microsoft sein bereits seit langem am Markt befindliches Client-Betriebssystem "Windows" an eine neue Microsoft-Unternehmensstrategie angepasst. Verändert hat sich insbesondere die Designphilosophie, weg vom bisherigen Prinzip des „lokalen Betriebssystems“ hin zu einer Dienstleistung („Windows as a Service“). Das bedeutet, dass das Betriebssystem neben den bisherigen lokalen Funktionen zusätzlich cloudbasierte Anwendungen enthält und deswegen auf eine enge Anbindung an die Cloud-Server-Infrastruktur von Microsoft angewiesen ist. Wichtige neue Aspekte im Vergleich zu den bisherigen Windows-Versionen sind vor allem der tief verankerte und teilweise nicht beeinflussbare Datenaustausch zwischen den Windows-Clients und der weltweiten Microsoft-Infrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur (bspw. Authentisierung via Azure oder Threat-Protection via Microsoft Defender ATP) in die Cloud. Diese Neuerungen sollten vor dem Einsatz von Windows 10 unbedingt berücksichtigt werden, insbesondere da nicht alle Funktionen in jeder angebotenen Windows Version zur Verfügung stehen bzw. nicht gewollte Funktionen sich deaktivieren lassen.

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 Windows 10 verarbeitet oder mit diesen übertragen werden. Die Sicherheitsrichtlinie zielt außerdem darauf ab, Geschäftsprozesse und andere IT-Systeme davor zu schützen, durch Windows-Systeme beeinträchtigt zu werden. Dazu müssen IT-Systeme mit dem Betriebssystem "Windows" angemessen abgesichert werden. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine SYS.2.1 "Allgemeiner Client" und SYS.2.2.3 "Clients unter Windows 10" 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 „Windows-Clients“ 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 „Windows-Clients"

## 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.

### Client unter Windows 10

#### Planung des Einsatzes von Cloud-Diensten unter Windows 10 (SYS.2.2.3.A1)

Workstations oder Notebooks mit dem Betriebssystem "Windows 10" sind eng mit den Cloud-Diensten des Herstellers Microsoft verzahnt. Es muss daher vor der Verwendung von Cloud-Diensten strategisch festgelegt werden, welche Cloud-Services in welchem Umfang genutzt werden sollen bzw. dürfen. Bei der strategischen Festlegung sind die benötigten Schutzbedürfnisse der verarbeiteten Daten der <Institution>, die Daten der Kunden sowie die etablierte Infrastruktur mit zu berücksichtigen.

#### Auswahl und Beschaffung einer geeigneten Windows 10-Version (SYS.2.2.3.A2)

Unter Berücksichtigung des benötigten Schutzbedürfnisses der verarbeiteten Daten der <Institution>, der Daten der Kunden und des Einsatzzwecks ist die benötigte "Windows 10" Version auszuwählen. Ebenfalls sind bei der Auswahl der Funktionsumfang und die Versorgung mit funktionalen Änderungen von "Windows 10" zu beachten.

Wurde sich für eine Version entschieden, ist die Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen zu prüfen. Basierend auf dem Ergebnis der Überprüfung ist der etablierte Beschaffungsprozess um die Auswahl des entsprechenden Lizenzmodells (Editionen Home, Enterprise, Education, Pro Education und Pro for Workstations) und „Service Branches“ (Current-Branch (CB), Current Branch for Business (CBB) oder Long Term Servicing Branch (LTSB)) zu erweitern.

#### Telemetrie und Datenschutzeinstellungen unter Windows 10 (SYS.2.2.3.A4)

Durch geeignete Maßnahmen auf Netzebene oder innerhalb des Betriebssystems "Windows 10" ist sicherzustellen, dass Daten der Telemetrie-, Nutzungs- und Diagnosedaten nicht an die Firma Microsoft übertragen werden.

#### Schutz vor Schadsoftware unter Windows 10 (SYS.2.2.3.A5)

Sofern nicht gleich- oder höherwertige Maßnahmen zum Schutz der Workstation oder dem Notebook sowie dem Betriebssystem vor einer Infektion mit Schadsoftware getroffen wurden, muss der Einsatz einer spezialisierten Komponente zum Schutz vor Schadsoftware auf Ebene des Betriebssystems "Windows 10" umgesetzt werden.

Für die Absicherung des Betriebssystems werden seitens des Herstellers Microsoft in Abhängigkeit der Version von "Windows 10" nachfolgend aufgelistete Technologien angeboten:

* AppLocker
* SecureBoot
* TPM
* Virtual Secure Mode (VSM)
* Encrypting File System (EFS)
* SmartScreen
* Microsoft Defender Anti-Treat-Protection

#### Integration von Online-Konten in das Betriebssystem (SYS.2.2.3.A6)

Bei der Auswahl der zu verwendenden "Windows 10" Version ist zu beachten, dass die Anmeldung nicht mit einem Microsoft-Konto (früher Microsoft Wallet, Microsoft Passport, .NET Passport, Microsoft Passport-Netzwerk und zuletzt Windows Live ID) erfolgen soll. Anmeldungen am System mit einem lokalen Benutzerkonto sollten nur Administratoren vorbehalten sein.

Konten anderer Anbieter von Identitätsmanagementsystemen für die Online-basierte Anmeldung am Windows-System, sollten nur mit zusätzlichen 2FA erfolgen. Grundsätzlich müssen alle genutzten Identitätsmanagementsysteme mit den gesetzlichen Anforderungen des Datenschutzes, den internen Sicherheitsvorgaben sowie den Bedürfnissen aus dem Notfallmanagement vereinbar sein.

## 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.

### Client unter Windows 10

#### Lokale Sicherheitsrichtlinien für Windows 10 (SYS.2.2.3.A7)

Alle sicherheitsrelevanten Einstellungen des "Windows 10" Systems sind bedarfsgerecht zu konfigurieren, zu testen und regelmäßig auf notwendige Anpassungen oder nach einem Funktionsupdate (Funktionsupdates werden für Windows 10 zweimal im Jahr (im März und September) bereitgestellt) zu überprüfen. Die Group Policy Object (GPO) Parameter sollten gemäß den Empfehlungen des Herstellers Microsoft, den Empfehlungen von Sicherheitsstandards (Hardening-Guides) bzw. führenden Sicherheitsexperten, dem benötigten Schutzbedarf und der benötigten Benutzerfreundlichkeit konfiguriert werden.

Abweichungen vom etablierten Absicherungsstandard sind zu dokumentiert und zu begründen. Alle nicht benötigten Anwendungen und Komponenten sollten deaktiviert werden.

Um zu verhindern, dass das Verhalten von "Windows 10" sich nach einem Funktionstüchtigen- oder Windowsupdate verändert, sollten in jedem Fall die benötigten GPO Parameter gesetzt werden, auch wenn die vorgenommen Einstellung dem aktuellen Standardverhalten (Werkseinstellungen von Microsoft) entspricht.

#### Zentrale Verwaltung der Sicherheitsrichtlinien von Clients (SYS.2.2.3.A8)

Alle GPO Parameter für "Windows 10" sollten durch ein zentrales Management verwaltet werden. Das zentrale Management sollte mittels dem von der Firma Microsoft bereitgestellten domänenweiten Gruppenrichtlinieneditor oder einer Mobile-Device-Management-Lösung unter Berücksichtigung des benötigten Schutzbedarf sowie den internen Richtlinien der <Institution> etabliert werden. Technisch nicht umsetzbare Konfigurationsparameter sollten dokumentiert, begründet und mit dem <Datenschutzbeauftragter>und <Informationssicherheitsbeauftragter> abgestimmt werden.

#### Sichere zentrale Authentisierung in Windows-Netzen (SYS.2.2.3.A9)

Für die zentrale Authentisierung am "Windows 10" Client sollte ausschließlich Kerberos in Version 5 oder SAML in Version 2 eingesetzt werden. Die eingesetzten kryptografischen Mechanismen sind entsprechend dem ermittelten Schutzbedarf und basierend auf den internen Richtlinien der <Institution> zu konfigurieren. Sofern Abweichungen von den freigegeben kryptographischen Mechanismen benötigt werden, sind diese zu beantragen.

Mittels GPO's sind die freigebenden kryptographischen Mechanismen und deren Parameter einzustellen und als nicht mehr sicher eingestufte Protokolle zu deaktivieren.

Die Authentisierung mittels LAN-Manager und NTLMv1 ist innerhalb der Infrastrukturen der <Institution> verboten.

#### Konfiguration zum Schutz von Anwendungen unter Windows 10 (SYS.2.2.3.A10)

Data Execution Prevention (DEP) sollte für alle Programme und Dienste im Opt-Out-Modus aktiviert werden (Opt-Out-Modus).

#### Schutz der Anmeldeinformationen unter Windows 10 (SYS.2.2.3.A11)

Die Funktion Virtual Secure Mode (VSM) sollte auf allen Hardware Clients unter "WINDOWS 10" aktiviert werden. Zusätzlich SOLLTE der Windows Defender Credential Guard gegen Angriffe auf die im System gespeicherten Authentisierungstoken und -hashes aktiviert werden. Sofern der Windows Defender Credential Guard nicht genutzt werden kann, sollte der Schutz des Local Credential Store LSA (Protected Mode Light) aktiviert werden.

Die Netzanmeldung von lokalen Konten ist verboten.

#### Datei- und Freigabeberechtigungen unter Windows 10 (SYS.2.2.3.A12)

Die Berechtigungen und der Zugriff auf Dateien und Ordner auf dem lokalen Windows-System sowie auf die Netzfreigaben sollte nach dem Need-to-Know-Prinzip erfolgen. Auch die standardmäßig vorhandenen administrativen Freigaben und Berechtigungen auf dem Windows-System sind hierbei zu berücksichtigen. Die Schreibrechte für Benutzer (Mitarbeitende) sind auf einen definierten Bereich im Windows Dateisystem zu beschränken. Insbesondere ist sicherzustellen, das Benutzer ohne administrative Rechte keine Schreibrechte für die Ordner des Betriebssystems oder der installierten Anwendungen erhalten bzw. besitzen.

#### Einsatz der SmartScreen-Funktion (SYS.2.2.3.A13)

Sofern die Workstations oder Notebooks mit dem Betriebssystem "Windows 10" nicht permanent mit der etablierten Anti-Threat-Infrastruktur der <Institution> verbunden sind, sollte die SmartScreen-Funktion aktiviert werden. Bei der Nutzung von SmartScreen werden unter Umständen personenbezogene Daten an Microsoft übertragen. Sofern dies nicht mit den internen Sicherheitsvorgaben oder gesetzlichen Datenschutzanforderungen vereinbar ist, sollte die SmartScreen-Funktion deaktiviert werden.

#### Einsatz des Sprachassistenten Cortana (SYS.2.2.3.A14)

Der Sprachassistent "Cortana" sollte auf den Windows-Systemen vollständig deaktiviert werden.

#### Einsatz der Synchronisationsmechanismen unter Windows 10 (SYS.2.2.3.A15)

Unter Berücksichtigung des Schutzbedarfes der Daten der Benutzer (Mitarbeitenden) und der Daten der Kunden der <Institution> sollte die Synchronisierung mit den Microsoft Cloud-Diensten deaktiviert werden. Das Sharing von WiFi-Passwörtern ist vollständig zu deaktivieren, denn allen Mitarbeitenden werden die benötigten WiFi-Passwörter über entsprechende Konfigurationsprofile bzw. dem Passwortmanager "1Password" zentral bereitgestellt.

#### Anbindung von Windows 10 an den Microsoft-Store (SYS.2.2.3.A16)

Die direkte Installation von Apps aus dem Windows-AppStore sollte für den Mitarbeitenden unterbunden werden. Sofern Mitarbeitende Anwendungen aus dem Windows-AppStore für den beruflichen Alltag benötigen, ist diese über den etablierten Bestellprozess zu beantragen.

#### Keine Speicherung von Daten zur automatischen Anmeldung (SYS.2.2.3.A17)

Die Speicherung von Kennwörtern, Zertifikaten und anderen Informationen zur automatischen Anmeldung an Webseiten und IT-Systemen sollte ohne zusätzlichen 2FA nicht genutzt werden.

#### Einsatz der Windows-Remoteunterstützung (SYS.2.2.3.A18)

Bei der Planung und Freigabe der Windows-Remoteunterstützung (hiermit ist nicht RDP gemeint) sind die Auswirkungen auf die Konfiguration der lokalen Firewall zu berücksichtigen. Eine Remoteunterstützung sollte nur nach einer expliziten Einladung durch den Mitarbeitenden erfolgen. Sofern die Einladung zur Remoteunterstützung in einer Datei gespeichert wird, muss diese Datei ein Kennwort besitzen.

Der aktuell am Windows-System angemeldete Benutzer (Mitarbeitende) muss dem Aufbau einer Sitzung für die Remoteunterstützung immer explizit zustimmen. Die maximale Gültigkeit der Einladung für eine Unterstützung aus der Ferne sollte die Dauer von 4 Stunden nicht überschreiten. Sofern die Windows-Remoteunterstützung innerhalb der <Institution> nicht verwendet wird, sollte diese vollständig deaktiviert werden.

#### Sicherheit beim Fernzugriff über RDP (SYS.2.2.3.A19)

Die Auswirkungen auf die Konfiguration der lokalen Firewall sind bei der Planung und Implementierung des Fernzugriffes mittels Remote Desktop Protocol (RDP) zu berücksichtigen. Die Gruppe der berechtigten Benutzer für die Nutzung von RDP sollte durch die Zuweisung entsprechender Benutzerrechte festgelegt werden. Per Default besitzt nur die Gruppe der Administratoren die Berechtigung für RDP. Idealerweise basiert die Zuweisung auf Basis von bereits etablierten Konzepten aus dem Microsoft-Directory (Active-Directory oder AzureAD) oder einem anderen Verzeichnisdienst.

Sollten erhöhte Schutzbedürfnisse des Zielsystems erfüllt werden müssen, sollte das RDP-Zielsystem nur durch ein dazwischengeschaltetes RDP-Gateway erreicht werden können.

Für die Verwendung von RDP ist zu prüfen, ob die nachfolgend aufgeführten Komfortfunktionen im Einklang mit dem Schutzbedarf des Zielsystems stehen:

* Die Verwendung der Zwischenablage,
* Die Einbindung von Druckern,
* Die Einbindung von Wechselmedien und Netzlaufwerken
* Die Nutzung der Dateiablagen und Smartcard-Anschlüssen

Sofern der Einsatz von RDP innerhalb der <Institution> nicht vorgesehen ist, sollte der RDP-Service vollständig deaktiviert werden.

Es sind die innerhalb der <Institution> freigegebenen kryptographischen Protokolle und Algorithmen für RDP einzusetzen.

#### Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten (SYS.2.2.3.A20)

Die Konfigurationsparameter der User Account Control (UAC) sollten für die privilegierten Konten (Domain Administrators, Enterprise Administrators, Schema Administrators, Account Operators, Backup Operators und BUILTIN\Administrators, Service Accounts für Softwareinstallationen und Updates und Service Accounts für Security Scans und Antivirussoftware) zwischen Bedienbarkeit und Sicherheitsniveau abgewogen eingesetzt werden. Die verwendenden Konfigurationsparameter sollten dokumentiert werden. Die Dokumentation sollte auch alle Konten mit Administratorrechten enthalten. In regelmäßig Abständen sollte geprüft werden, ob die Dokumentation noch auf dem aktuellen Stand ist und bei Bedarf aktualisiert 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.

### Client unter Windows 10

#### Einsatz des Encrypting File Systems (EFS) (SYS.2.2.3.A21 - CI)

Da das Encrypting File System (EFS) die verwendeten Schlüssel mit dem Passwort des Benutzerkontos schützt, ist ein komplexes Passwort zu verwenden. Zusätzlich sollten restriktive Zugriffsrechte die mit EFS verschlüsselten Dateien und Ordner schützen. An Stelle des Benutzerkonto "Administrator" sollte ein dediziertes Konto für den Wiederherstellungsagenten verwendet werden. Beim Einsatz von EFS mit lokalen Benutzerkonten anstatt Domänenkontos sollten die lokalen Passwortspeicher mittels BitLocker übergreifend verschlüsselt werden.

Hieraus ableitend, sollte vor der Inbetriebnahme von EFS für die Verschlüsselung von Dateien und Ordner folgende Themenblöcke geplant und in einem Konzept geregelt und dokumentiert werden:

* Zweck des Einsatzes von EFS
* Verträglichkeit mit anderen bereits im Einsatz befindliche Lösungen
* Berechtigungen der Benutzer und Administratoren auf die folgenden Pfade und darin enthaltenen Dateien:
	+ %APPDATA% | Microsoft | Crypto | RSA
	+ %APPDATA% | Microsoft | Protect
* Ablageort der Wiederherstellungsinformationen
* Wiederherstellungsinformationen und der berechtigte Benutzerkreis

Im Rahmen des etablierten Schulungsprogramms sollten die Mitarbeitenden im korrekten Umgang mit EFS geschult werden.

#### Verwendung der Windows PowerShell (SYS.2.2.3.A22 - CI)

Beim Betriebssystem "Windows 10" lassen sich die Funktionen PowerShell-Skriptumgebung nur noch für die Version 2.0 entfernen, sofern gleichzeitig das .NET-Framework deinstalliert wird. Hieraus ableitend sollte die Ausführung der WPS-Dateien nur den Benutzern mit administrativen Rechten gestattet werden.

Die Ausführung von PowerShell sollte zentral protokolliert und die Protokolle sollten kontinuierlich überwacht werden. Um zu verhindern, dass unsignierte Skripte versehentlich ausgeführt werden, sollte die Ausführung von PowerShell-Skripten mit dem Befehl Set-ExecutionPolicy AllSigned eingeschränkt werden.

#### Erweiterter Schutz der Anmeldeinformationen unter Windows 10 (SYS.2.2.3.A23 - CIA)

Auf UEFI-basierten Systemen sollte SecureBoot verwendet und der Status des geschützten Modus für den Local Credential Store LSA beim Systemstart überwacht werden (siehe auch Abschnitt "Schutz der Anmeldeinformationen unter Windows 10"). Beim Einsatz von "Windows 10" in einer Windows-Domäne und einem Active-Directory ab dem Funktionslevel "2012 R2" ist die Option „restrictedAdmin“ für den Service RDP zu aktivieren.

#### Aktivierung des Last-Access-Zeitstempels (SYS.2.2.3.A24 - C)

Zur leichteren Identifikation eines Systemmissbrauchs sollte der Last-Access-Zeitstempel von NTFS aktiviert werden. Vor der Aktivierung ist zu prüfen, welche Auswirkungen sie auf die Systemleistung hat. Die Ergebnisse der Überprüfung und die Entscheidung über die Aktivierung sollten dokumentiert werden.

#### Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“ (SYS.2.2.3.A25 - CIA)

Es sollte beim Einsatz von "Windows 10" berücksichtigt werden, dass die Komponente „Connected User Experience and Telemetry“ (CUET) ein fester Bestandteil des Betriebssystems ist und neben der Telemetriefunktion auch eine Möglichkeit des Fernzugriffes für den Hersteller Microsoft auf die Workstation oder Notebook erlaubt. Ein solcher Fernzugriff sollte netzseitig protokolliert werden und sollte über die Infrastruktur der <Institution> geblockt werden.