Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.2.3 Clients unter Windows

1. Beschreibung

1.1. Einleitung

Mit Windows 10 hat Microsoft sein Client-Betriebssystem Windows an eine neue Unternehmensstrategie angepasst. Verändert hat sich insbesondere auch die grundlegende Philosophie, weg vom bisherigen Prinzip des „lokalen Betriebssystems“ hin zu einer Dienstleistung („Windows as a Service“). Das bedeutet, dass das Betriebssystem neben den bisherigen Funktionen auch darüber hinausgehende, insbesondere cloudbasierte, Anwendungen enthält und deswegen auf eine enge Anbindung an die 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 Clients und der Herstellerinfrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur (z. B. Authentisierung) in die Cloud.

Mit Windows 11 wurde im Oktober 2021 eine Nachfolgeversion veröffentlicht. Diese enthält neue Funktionen, hat eine überarbeitete Bedienoberfläche und im Vergleich zu Windows 10 deutlich erhöhte Systemvoraussetzungen. Insbesondere setzt Windows 11 offiziell eine 64-Bit-fähige CPU, UEFI SecureBoot sowie ein TPM 2.0 voraus. Windows 11 ist trotz des Versionssprungs jedoch keine komplette Neuentwicklung, sondern basiert auf Windows 10. Dieser Baustein ist daher sowohl für Windows 10 als auch für Windows 11 anwendbar.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows-Clients mit Windows 10 oder 11 verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.2.3 *Clients unter Windows* ist für alle Clients anzuwenden, auf denen das Betriebssystem Microsoft Windows 10 oder 11 eingesetzt wird.

Dieser Baustein enthält spezifische Anforderungen, die zum sicheren Betrieb von Clients unter dem Betriebssystem Windows zusätzlich zu den Anforderungen aus dem Baustein SYS.2.1 *Allgemeiner Client* zu beachten und zu erfüllen sind. Für Anwendungsprogramme, die auf den Windows-Clients verwendet werden, sind die Anforderungen der entsprechenden Bausteine zu erfüllen, beispielsweise APP.1.1 *Office-Produkte* oder APP.1.2 *Webbrowser*. Beim Einsatz in einer Windows-Domäne sind die

Anforderungen der entsprechenden Bausteine wie APP.2.2 *Active Directory Domain Services* zu erfüllen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.2.3 *Clients unter Windows* von besonderer Bedeutung.

2.1. Schadprogramme auf Windows-Clients

Aufgrund der hohen Verbreitung von Windows-Betriebssystemen und der zwischen den Systemgenerationen oftmals vorhandenen Abwärtskompatibilität zu älteren Versionen ist die Gefährdung durch Schadprogramme und unbefugtes Eindringen in IT-Systeme für Windows vergleichsweise hoch.

2.2. Integrierte Cloud-Funktionen

Windows beinhaltet zahlreiche Funktionen, mit denen Daten unter Nutzung der Dienste von Microsoft abgelegt und synchronisiert werden („Cloud-Dienste“). Dadurch besteht die Gefahr, diese unbewusst, oder zumindest unbedacht, auch für möglicherweise institutionskritische oder personenbezogene Daten zu nutzen. Außerdem können Benutzende gegen die Datenschutzgesetze verstoßen, wenn Daten bei Dritten, in der Regel im Ausland, gespeichert werden. Meldet sich eine Person mit bereits aktiviertem Microsoft-Account an ein neues Gerät an, werden automatisch die von ihm genutzten Microsoft-Cloud-Dienste eingerichtet. So können Daten der Institution ungewollt auf die privaten Geräte der Mitarbeitenden synchronisiert werden. Als weiteres Beispiel bietet Windows als Standardeinstellung die Möglichkeit, den Bitlocker-Recovery-Schlüssel direkt über den Microsoft-Account in der Cloud zu sichern und somit schutzbedürftige kryptografische Geheimnisse in die Hände Dritter zu geben.

2.3. Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme

Software, die auf Vorgängerversionen eines Betriebssystems erfolgreich betrieben werden konnte, muss nicht auch grundsätzlich mit der aktuellen Version von Windows zusammenarbeiten. Mögliche Ursachen sind neue Sicherheitsmerkmale oder Betriebssystemeigenschaften sowie der Wegfall von Funktionen oder Diensten. In der Folge kann die Software nicht oder nur eingeschränkt verwendet werden. Beispiele für aktivierte Sicherheitsmerkmale, die bei neuen Windows-Versionen die Ursache für mögliche Kompatibilitätsprobleme sein können, sind die Benutzerkontensteuerung (UAC) oder, bei 64-Bit-Versionen des Betriebssystems, Kernel Patch Guard. Außerdem könnten signierte Treiber notwendig sein, die möglicherweise für ältere Geräte nicht mehr zur Verfügung stehen.

2.4. Telemetrie-Funktionen von Windows

Windows sendet standardmäßig sogenannte Diagnosedaten an den Hersteller Microsoft. Zusätzlich kann Microsoft über den in Windows integrierten Telemetrie-Dienst gezielt Informationen von einem Client abfragen. Im Telemetrie-Level „Full“ bzw. „Vollständig“, der in den Windows-Editionen Home und Pro der Standard-Level ist, schließt dies beispielsweise den Zugriff auf die Registry des Clients sowie die Ausführung von bestimmten Diagnosetools auf dem Client mit ein. Es besteht die Gefahr, dass die Diagnose- bzw. Telemetriedaten schützenswerte Informationen enthalten, die auf diesem Weg an Dritte gelangen können.

2.5. Eingeschränkte Forensik bei der Nutzung des Virtual Secure Mode (VSM)

Durch die Nutzung des Virtual Secure Mode (VSM) werden forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt bzw. erschwert. Prozesse, die durch den Secure Kernel bzw. dem Isolated User Mode (IUM) geschützt werden, sind nicht mehr zugänglich. Beispielsweise können Speicherabbilder dieser Prozesse aufgrund kryptografischer Maßnahmen nicht ausgewertet werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.2.3 *Clients unter Windows* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

Da Windows-basierte Geräte eng mit den Cloud-Diensten des Herstellers Microsoft verzahnt sind, MUSS vor ihrer Verwendung strategisch festgelegt werden, welche enthaltenen Cloud-Dienste in welchem Umfang genutzt werden sollen bzw. dürfen.

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

Der Funktionsumfang und die Versorgung mit funktionalen Änderungen einer Windows-Version MÜSSEN unter Berücksichtigung des ermittelten Schutzbedarfs und des Einsatzzwecks ausgewählt werden. Die Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen MUSS bei der Auswahl berücksichtigt werden. Basierend auf dem Ergebnis der Überprüfung MUSS der etablierte Beschaffungsprozess um die Auswahl des entsprechenden Lizenzmodells und „Service Branches“ (CB, CBB oder LTSC) erweitert werden.

SYS.2.2.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen unter Windows (B)

Um die Übertragung von Diagnose- und Nutzungsdaten an Microsoft stark zu reduzieren, MUSS das Telemetrie-Level 0 (Security) in der Enterprise-Edition von Windows konfiguriert werden. Wenn diese Einstellung nicht wirksam umgesetzt wird oder bei anderen Windows-Edition umgesetzt werden

kann, dann MUSS durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass die Daten nicht an den Hersteller übertragen werden.

SYS.2.2.3.A5 Schutz vor Schadsoftware unter Windows (B)

Sofern nicht gleich- oder höherwertige Maßnahmen, wie z. B. Ausführungskontrolle, zum Schutz des IT-Systems vor einer Infektion mit Schadsoftware getroffen wurden, MUSS eine spezialisierte Komponente zum Schutz vor Schadsoftware auf Windows-Clients eingesetzt werden.

SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem (B) [Benutzende]

Die Anmeldung am System sowie an der Domäne DARF NUR mit dem Konto eines selbst betriebenen Verzeichnisdienstes möglich sein. Anmeldungen mit lokalen Konten SOLLTEN Administrierenden vorbehalten sein. Online-Konten zur Anmeldung, etwa ein Microsoft-Konto oder Konten anderer Identitätsmanagementsysteme, DÜRFEN NICHT verwendet werden, da hier personenbezogene Daten an die Systeme Dritter übertragen werden.

3.2. Standard-Anforderungen

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

SYS.2.2.3.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.3.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

Für die zentrale Authentisierung SOLLTE ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie SOLLTE die Verwendung älterer Protokolle verhindern. Ist dies nicht möglich, MUSS alternativ NTLMv2 eingesetzt werden. Die Authentisierung mittels LAN-Manager und NTLMv1 DARF NICHT innerhalb der Institution und in einer produktiven Betriebsumgebung erlaubt werden. Die eingesetzten kryptografischen Mechanismen SOLLTEN entsprechend dem ermittelten Schutzbedarf und basierend auf den internen Richtlinien konfiguriert und dokumentiert werden. Abweichende Einstellungen SOLLTEN begründet und mit dem Sicherheitsmanagement abgestimmt sein.

SYS.2.2.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.3.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

Der Zugriff auf Dateien und Ordner auf dem lokalen System sowie auf Netzfreigaben SOLLTE gemäß einem Berechtigungs- und Zugriffskonzept konfiguriert werden. Auch die standardmäßig vorhandenen administrativen Freigaben auf dem System SOLLTEN hierbei berücksichtigt werden. Die Schreibrechte für Benutzende SOLLTEN auf einen definierten Bereich im Dateisystem beschränkt werden. Insbesondere SOLLTEN Benutzende keine Schreibrechte für Ordner des Betriebssystems oder installierter Anwendungen erhalten.

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

Die SmartScreen-Funktion, die aus dem Internet heruntergeladene Dateien und Webinhalte auf mögliche Schadsoftware untersucht und dazu unter Umständen personenbezogene Daten an Microsoft überträgt, SOLLTE deaktiviert werden.

SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana (S) [Benutzende]

Cortana SOLLTE deaktiviert werden.

SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen unter Windows (S)

Die Synchronisierung von Benutzendendaten mit Microsoft Cloud-Diensten und das Sharing von WLAN-Passwörtern SOLLTEN vollständig deaktiviert werden.

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

Die Verwendung des Microsoft-Stores SOLLTE auf die Verträglichkeit mit den Datenschutz- und Sicherheitsvorgaben der Institution überprüft und bewertet werden. Die generelle Installation von Apps auf Windows ist nicht von der Anbindung an den Microsoft-Store abhängig, daher SOLLTE sie, sofern sie nicht benötigt wird, deaktiviert werden.

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

Die Speicherung von Kennwörtern, Zertifikaten und anderen Informationen zur automatischen Anmeldung an Webseiten und IT-Systemen SOLLTE NICHT erlaubt werden.

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

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung der Windows-Remoteunterstützung (hiermit ist nicht RDP gemeint) berücksichtigt werden. Eine Remoteunterstützung SOLLTE nur nach einer expliziten Einladung erfolgen. Bei der Speicherung einer Einladung in einer Datei SOLLTE diese ein Kennwort besitzen. Dem Aufbau einer Sitzung SOLLTE immer explizit zugestimmt werden. Die maximale Gültigkeit der Einladung für eine Unterstützung aus der Ferne SOLLTE in der Dauer angemessen sein. Sofern die Windows-Remoteunterstützung nicht verwendet wird, SOLLTE sie vollständig deaktiviert werden.

SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP (S) [Benutzende]

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der berechtigten Benutzenden für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Berechtigungen festgelegt werden. In komplexen Infrastrukturen SOLLTE das RDP-Zielsystem nur durch ein dazwischengeschaltetes RDP-Gateway erreicht werden können. Für die Verwendung von RDP SOLLTE eine Prüfung und deren Umsetzung sicherstellen, dass 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 sowie
- die Nutzung der Dateiablagen und von Smartcard-Anschlüssen.

Sofern der Einsatz von Remote-Desktopzugriffen nicht vorgesehen ist, SOLLTEN diese vollständig deaktiviert werden. Die eingesetzten kryptografischen Protokolle und Algorithmen SOLLTEN sicher sein und den internen Vorgaben der Institution entsprechen.

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

Die Konfigurationsparameter der sogenannten Benutzerkontensteuerung (User Account Control, UAC) SOLLTEN für die privilegierten Konten zwischen Bedienbarkeit und Sicherheitsniveau abgewogen eingesetzt werden. Die Entscheidungen für die zu verwendenden Konfigurationsparameter SOLLTEN dokumentiert werden. Darüber hinaus SOLLTE die Dokumentation alle Konten mit Administrationsrechten enthalten sowie regelmäßig geprüft werden, ob es notwendig ist, die Rechte erweitern zu können.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.2.3.A21 Einsatz des Encrypting File Systems (H)

Da das Encrypting File System (EFS) die verwendeten Schlüssel mit dem Passwort des jeweiligen Kontos schützt, SOLLTE ein sicheres Passwort verwendet werden. Zusätzlich SOLLTEN restriktive Zugriffsrechte die mit EFS verschlüsselten Dateien schützen. Der Wiederherstellungsagent SOLLTE ein dediziertes Konto und kein Administrationskonto sein. In diesem Zusammenhang SOLLTE der private Schlüssel des Agenten gesichert und aus dem System entfernt werden. Es SOLLTEN von allen privaten Schlüsseln Datensicherungen erstellt werden. Beim Einsatz von EFS mit lokalen Konten SOLLTEN die lokalen Passwortspeicher mittels Syskey verschlüsselt werden. Alternativ kann der Windows Defender Credential Guard genutzt werden. Benutzende SOLLTEN im korrekten Umgang mit EFS geschult werden.

SYS.2.2.3.A22 Verwendung der Windows PowerShell (H)

Die PowerShell und die WPS-Dateien SOLLTEN NUR von Administrierenden ausgeführt werden können. Die PowerShell-Ausführung selbst SOLLTE zentral protokolliert und die Protokolle überwacht werden. Die Ausführung von PowerShell-Skripten SOLLTE mit dem Befehl *Set-ExecutionPolicy AllSigned* eingeschränkt werden, um zu verhindern, dass unsignierte Skripte versehentlich ausgeführt werden.

SYS.2.2.3.A23 Erweiterter Schutz der Anmeldeinformationen unter Windows (H)

Auf UEFI-basierten Systemen SOLLTE SecureBoot verwendet und der Status des geschützten Modus für den Local Credential Store LSA beim Systemstart überwacht werden. Ist eine Fernwartung der Clients mittels RDP vorgesehen, SOLLTE beim Einsatz von Windows in einer Domäne ab dem Funktionslevel 2012 R2 von der Option „restrictedAdmin“ für RDP Gebrauch gemacht werden.

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

Es SOLLTE geprüft werden, ob der Last-Access-Zeitstempel im Dateisystem aktiviert werden kann, um die Analyse eines Systemmissbrauchs zu erleichtern. Bei der Prüfung SOLLTEN mögliche Auswirkungen dieser Einstellung, wie Performance-Aspekte oder resultierende Einschränkungen bei inkrementellen Backups, berücksichtigt werden.

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

Es SOLLTE berücksichtigt werden, dass die Komponente „Connected User Experience and Telemetry“ (CUET) bei Windows fester Bestandteil des Betriebssystems ist und neben der Telemetriefunktion auch

eine Fernzugriffsmöglichkeit für den Hersteller Microsoft auf das lokale System erlaubt. Ein solcher Fernzugriff auf den Windows-Client SOLLTE netzseitig geloggt und falls erforderlich geblockt werden.

SYS.2.2.3.A26 Nutzung des Virtual Secure Mode (VSM) (H)

Bei der Nutzung des Virtual Secure Mode (VSM) SOLLTE berücksichtigt werden, dass forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt oder erschwert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI stellt im Rahmen des Projekts „SiSyPHuS Win10 (**S**tud**i**e zu **Sy**stemintegrität, **P**rotokollierung, **H**ärtung **u**nd **S**icherheitsfunktionen in Windows 10)“ eine Analyse der Sicherheitsfunktionen von Windows 10 und darauf aufbauend passende Härtungsempfehlungen bereit: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html

Der Hersteller Microsoft stellt unter anderem folgende weiterführende Informationen zu Windows bereit:

- Konfigurieren von zusätzlichem LSA-Schutz: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- Credential Guard - Überblick: https://docs.microsoft.com/de-de/windows/access-protection/credential-guard/credential-guard-requirements
- Device Guard - Überblick: https://technet.microsoft.com/de-de/library/dn986865.aspx