SYS.2.2.3 Clients unter Windows 10

# Beschreibung

## 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 des Herstellers 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. Diese Neuerungen sollten vor dem Einsatz von Windows 10 unbedingt berücksichtigt werden.

## Zielsetzung

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

## Abgrenzung und Modellierung

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

Dieser Baustein enthält spezifische Anforderungen, die zum sicheren Betrieb von Clients unter dem Betriebssystem Windows 10 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 *Web-Browser*. Beim Einsatz in einer Windows-Domäne sind die Anforderungen der entsprechenden Bausteine wie APP.2.2 *Active Directory* zu erfüllen.

# 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 10* von besonderer Bedeutung.

## Schadprogramme unter Windows 10

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 das IT-System vergleichsweise hoch. Schadprogramme können eine Vielzahl von Funktionen besitzen und einem Angreifer umfangreiche Steuerungsoptionen ermöglichen. Unter anderem können sie gezielt Passwörter auslesen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren. Besonders gravierend für eine Institution ist der Schaden, der durch den Verlust oder die Verfälschung von Informationen oder Anwendungen entsteht. Aber auch der Imageverlust sowie der finanzielle Schaden, der durch Schadprogramme entstehen kann, sind oft schwerwiegend.

## Integrierte Cloud-Funktionen

Windows 10 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 Benutzer gegen die Datenschutzgesetze verstoßen, wenn Daten bei Dritten, in der Regel im Ausland, gespeichert werden. Meldet sich ein Benutzer 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 Mitarbeiter synchronisiert werden. Als weiteres Beispiel bietet Windows 10 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.

## 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 10 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.

## Telemetrie-Funktionen von Windows 10

Windows 10 sendet standardmäßig sogenannte Diagnosedaten an den Hersteller Microsoft. Zusätzlich kann Microsoft über den in Windows 10 integrierten Telemetrie-Dienst gezielt Informationen von einem Client abfragen. Im Telemetrie-Level „Full“ bzw. „Vollständig“, der auf Windows 10 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.

## 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.

# Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.2.3 *Clients unter Windows 10* aufgeführt. Der ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der 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 | Benutzer |

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.

## 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 10 (B)

Da Windows-10-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-10-Version (B)

Der Funktionsumfang und die Versorgung mit funktionalen Änderungen einer Windows-10-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 10 (B)

Die Telemetriedienste übertragen Diagnose- und Nutzungsdaten, die der Hersteller zur Erkennung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Identifizierung mit eindeutigen Merkmalen verknüpft. Diese können nur unter Windows 10 Enterprise mit der Einstellung des Telemetrielevels 0 (Security) stark reduziert werden. Wenn diese Einstellung nicht wirksam umgesetzt werden kann, dann MUSS durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass diese Daten nicht an den Hersteller übertragen werden.

### SYS.2.2.3.A5 Schutz vor Schadsoftware unter Windows 10 (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 10-Clients eingesetzt werden.

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

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

## 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 10 (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 Benutzer SOLLTEN auf einen definierten Bereich im Dateisystem beschränkt werden. Insbesondere SOLLTEN Benutzer keine Schreibrechte für Ordner des Betriebssystems oder installierte 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 [Benutzer] (S)

Cortana SOLLTE deaktiviert werden.

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

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

### SYS.2.2.3.A16 Anbindung von Windows 10 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 10 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. Der aktuell angemeldete Benutzer SOLLTE dem Aufbau einer Sitzung immer explizit zustimmen. Die maximale Gültigkeit der Einladung für eine Unterstützung aus der Ferne SOLLTE in der Dauer angemessen sein. Sofern dieser Service nicht verwendet wird, SOLLTE er vollständig deaktiviert werden.

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

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Benutzerrechte 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 den internen Vorgaben der Institution entsprechen.

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

Die Konfigurationsparameter der 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 Administratorrechten enthalten sowie regelmäßig geprüft werden, ob es notwendig ist, die Rechte erweitern zu können.

## 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 Benutzerkontos schützt, SOLLTE ein sicheres Passwort verwendet werden. Zusätzlich SOLLTEN restriktive Zugriffsrechte die mit EFS verschlüsselten Dateien schützen. Der Wiederherstellungsagent SOLLTE ein dediziertes Konto und nicht der Administrator 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 Benutzerkonten SOLLTEN die lokalen Passwortspeicher mittels Syskey verschlüsselt werden. Alternativ kann der Windows Defender Credential Guard genutzt werden. Die Benutzer 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 Administratoren 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 10 (H)

Auf UEFI-basierten Systemen SOLLTE SecureBoot verwendet und der Status des geschützten Modus für den Local Credential Store LSA beim Systemstart überwacht werden (vgl. hierzu SYS.2.2.3.A11 *Schutz der Anmeldeinformationen unter Windows 10*). Ist eine Fernwartung der Clients mittels RDP vorgesehen, SOLLTE beim Einsatz von Windows 10 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)

Wird ein Sicherheitskonzept für ein IT-System mit Windows 10 erstellt, SOLLTE dabei 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 10 fester Bestandteil des Betriebssystems ist und neben der Telemetriefunktion auch eine Fernzugriffsmöglichkeit für den Betriebssystemhersteller auf das lokale System erlaubt. Ein solcher Fernzugriff auf den Windows 10-Client SOLLTE netzseitig geloggt und falls erforderlich geblockt werden.

# Weiterführende Informationen

## 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 u. a. folgende weiterführende Informationen zu Windows 10 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>

# Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Aus jeder Anforderung (A) in diesem Baustein können Sicherheitsmaßnahmen abgeleitet werden. Die Umsetzung dieser Maßnahmen wirkt denjenigen elementaren Gefährdungen (G0) entgegen, die für das Thema bzw. Zielobjekt relevant sind. In der Kreuzreferenztabelle (KRT) zu diesem Baustein sind jeder Anforderung die entsprechenden elementaren Gefährdungen zugeordnet.

Anhand der KRT lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Die Buchstaben in der zweiten Spalte zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Diese Grundwerte sind Confidentiality (C) für Vertraulichkeit, Integrity (I) für Integrität sowie Availability (A) für Verfügbarkeit.

Die folgenden elementaren Gefährdungen sind für den Baustein SYS.2.2.3 *Clients unter Windows 10* von Bedeutung:

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme