SYS.2.2: Windows-Clients

SYS.2.2.2: Clients unter Windows 8.1

1 Beschreibung

1.1 Einleitung

Mit Windows 8 hat Microsoft sein Client-Betriebssystem Windows sowie die damit eingeführten Funktionen und Komponenten weiterentwickelt. Neu an Windows 8 bzw. 8.1 ist eine Bedienführung, die auf den Einsatz mobiler Geräte mit Touchscreen ausgerichtet ist. Diese bringt ein neues Bedienkonzept für Anwendungen mit sich, neben den klassischen Desktop-Anwendungen hat Microsoft eine Klasse mobiler Anwendungen zur Nutzung vorgesehen, die sogenannten Apps. Diese sind konsequent auf die Steuerung durch Berührung ausgelegt. Zusätzlich können sie als „Kachel“ auf dem Bildschirm Anzeigefunktionen wahrnehmen. Einige Anwendungen, allen voran der mit Windows 8.1 ausgelieferte Internet Explorer, stehen entsprechend in zwei Varianten zur Verfügung, in der altbekannten Desktop-Version sowie in der neuen App-Version. Mit Windows 10 ist eine Nachfolge-Version für Windows 8.1 verfügbar. Der erweiterte Support für Windows 8.1 durch Microsoft endet am 10. Januar 2023.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die durch und auf Clients unter Windows 8.1 verarbeitet werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.2.2.2 *Clients unter Windows 8.1* ist für alle Client-Systeme anzuwenden, auf denen das Betriebssystem Microsoft Windows 8.1 eingesetzt wird.

Der vorliegende Baustein beschreibt Anforderungen, die für Windows 8.1 spezifisch sind. Die Anforderungen aus dem Baustein SYS.2.1 *Allgemeiner Client* sind in jedem Fall ebenfalls zu erfüllen. Für Anwendungsprogramme, die auf den Windows-Clients verwendet werden, sind die Anforderungen der entsprechenden Bausteine umzusetzen, 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.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.2.2.2 *Clients unter Windows 8.1* von besonderer Bedeutung:

2.1 Auf Windows ausgerichtete Schadprogramme

Microsoft Windows ist aufgrund seiner weiten Verbreitung ein beliebtes Ziel für verschiedenste Angriffe mit Schadprogrammen, sodass hier ein großes Gefährdungspotenzial besteht. Schadprogramme können viele unterschiedliche Funktionen haben und bieten einem Angreifer dadurch umfangreiche Kommunikations- und Steuerungsmöglichkeiten. Unter anderem können Schadprogramme 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.

2.2 Integrierte Cloud-Funktionen

Windows 8.1 bringt zahlreiche Funktionen mit, mit denen Daten in den Cloud-Diensten von Microsoft abgelegt und darüber synchronisiert werden. Dadurch besteht die Gefahr, Cloud-Dienste unbewusst (oder zumindest unbedacht) auch für möglicherweise institutionskritische oder personenbezogene Daten zu nutzen. Außerdem können Benutzer gegen Datenschutzgesetze verstoßen, wenn Daten bei Dritten, vor allem im Ausland, gespeichert werden. Meldet sich ein Benutzer mit bereits aktiviertem Microsoft-Account an ein neues Gerät an, werden dort 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 8.1 als Standardeinstellung die Möglichkeit, den Bitlocker-Recovery-Schlüssel direkt über den Microsoft-Account in der Cloud zu sichern. Damit werden schutzbedürftige, verschlüsselte Informationen in die Hände Dritter gegeben.

2.3 Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme

Software, die auf Windows-Vorgängerversionen erfolgreich betrieben wurde, muss nicht auch automatisch mit der aktuellen Version des Betriebssystems 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. Bei neuen Windows-Versionen kann beispielsweise die Aktivierung neuer Sicherheitsmerkmale zu Kompatibilitätsproblemen führen. Beispiele dafür sind die Benutzerkontensteuerung (UAC) oder, bei 64-Bit-Versionen des Betriebssystems, der Kernel Patch Guard. Außerdem können signierte Treiber notwendig sein, die eventuell für ältere Geräte nicht mehr verfügbar sind. Bei neueren Windows-Versionen kommt es auch immer wieder vor, dass Funktionen wegfallen. Ein Beispiel hierfür ist der Wegfall der GINA-Anmeldekomponente, die z. B. von einigen Fingerabdrucklesern verwendet wurde.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.2.2 *Clients unter Windows 8.1* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.2.2.2 *Clients unter Windows 8.1* vorrangig erfüllt werden:

SYS.2.2.2.A1 Auswahl einer geeigneten Windows 8.1-Version (B)

Bevor eine Windows 8.1-Version beschafft wird, MUSS eine geeignete Version ausgewählt werden, die alle notwendigen Funktionen für den zukünftigen Einsatz mitbringt. Es SOLLTEN bevorzugt 64-Bit-Versionen eingesetzt werden, die erweiterte Sicherheitsfeatures enthalten.

SYS.2.2.2.A2 Festlegung eines Anmeldeverfahrens für Windows 8.1 (B)

Abhängig von den Sicherheitsanforderungen MUSS entschieden werden, ob neben dem klassischen Anmeldeverfahren über ein Passwort auch andere Verfahren (z. B. über PIN) erlaubt sein sollen.

SYS.2.2.2.A3 Einsatz von Viren-Schutzprogrammen unter Windows 8.1 (B)

Sofern nicht gleich- oder höherwertige Maßnahmen zum Schutz des IT-Systems vor einer Infektion mit Schadsoftware getroffen wurden, MUSS ein Virenschutz-Programm auf den Clients unter Windows 8.1 eingesetzt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.2.2.2 *Clients unter Windows 8.1*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.2.2.A4 Beschaffung von Windows 8.1 (S)

Bei der Beschaffung von Windows 8.1 bzw. der entsprechenden Hardware für das Windows 8.1-System SOLLTEN die Anforderungen gemäß dem Windows Hardware Certification Requirement berücksichtigt werden. Des Weiteren SOLLTEN die zu beschaffenden Systeme über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot und, sofern vorhanden, für das TPM verfügen, die eine Kontrolle durch den Eigentümer ermöglicht. Außerdem SOLLTE ein geeignetes Lizenzmodell ausgewählt werden.

SYS.2.2.2.A5 Lokale Sicherheitsrichtlinien für Windows 8.1 (S)

Es SOLLTEN alle sicherheitsrelevanten Einstellungen über entsprechende Sicherheitsrichtlinien bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Die Verteilung der Sicherheitseinstellungen auf mehrere Windows 8.1-Clients SOLLTE entsprechend den spezifischen Gegebenheiten der Institution erfolgen.

SYS.2.2.2.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.2.A7 Einsatz der Windows-Benutzerkontensteuerung UAC (S)

Um eine restriktive Rechtevergabe zu unterstützen, SOLLTE die Benutzerkontensteuerung (User Account Control, UAC) aktiviert sein. Für Standardbenutzer SOLLTE festgelegt sein, dass die Aufforderung zur Passworteingabe für erhöhte Rechte automatisch abgelehnt wird. Für Administratorenkonten SOLLTE die Einstellung von UAC zwischen Bedienbarkeit und Sicherheitsniveau abgewogen werden. Die Entscheidung SOLLTE dokumentiert und die entsprechenden Einstellungen konfiguriert werden. Es SOLLTE regelmäßig geprüft werden, ob die jeweiligen Rechte noch notwendig sind und diese entsprechend angepasst oder entzogen werden.

SYS.2.2.2.A8 Keine Verwendung der Heimnetzgruppen-Funktion [Benutzer] (S)

Clients SOLLTEN KEINE Dienste wie Datei- oder Druckerfreigaben anbieten. Eine Sicherheits- bzw. Gruppenrichtlinie (Group Policy Object, GPO) mit der Einstellung „Beitritt des Computers zu einer Heimnetzgruppe verhindern“ SOLLTE für alle Clients gelten. Wird die Funktion aus betrieblichen Gründen eingesetzt, SOLLTEN die Benutzer im Umgang mit den Freigaben der Heimnetzgruppe geschult werden.

SYS.2.2.2.A9 Datenschutz und Datensparsamkeit bei Windows 8.1-Clients [Benutzer] (S)

Werden Microsoft-Konten für die Benutzer angelegt, SOLLTEN nur unbedingt erforderliche Angaben zu den Personen hinterlegt werden. 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. Bevor eine Anwendung oder App zur Nutzung innerhalb der Institution freigegeben wird, SOLLTE sorgfältig geprüft werden, welche Daten diese Anwendungen automatisch an die Microsoft-Cloud übersenden. Anwendungen SOLLTEN so konfiguriert werden, dass keine schützenswerten Daten übertragen werden. Apps, die unerwünschte oder unnötig umfangreiche Daten an Dritte übertragen, SOLLTEN nicht verwendet werden.

SYS.2.2.2.A10 Integration von Online-Konten in das Betriebssystem [Benutzer] (S)

Die Anmeldung am IT-System und an der Domäne SOLLTE nur mit einem Konto eines selbst betriebenen Verzeichnisdienstes, wie z. B. Active Directory, möglich sein. Eine lokale Anmeldung SOLLTE Administratoren vorbehalten sein. Werden zur Anmeldung Online-Konten, wie z. B. ein Microsoft-Konto oder Konten anderer Anbieter von Diensten zum Identitätsmanagement, verwendet, SOLLTE darauf geachtet werden, dass der Anbieter vertrauenswürdig ist und der Datenschutz eingehalten wird.

SYS.2.2.2.A11 Konfiguration von Synchronisationsmechanismen in Windows 8.1 (S)

Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten SOLLTE vollständig deaktiviert werden.

SYS.2.2.2.A12 Sichere zentrale Authentisierung in Windows-Netzen (S)

In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie SOLLTE die Verwendung älterer Protokolle verhindern. Der Schutz des Local Credential Store (LSA) SOLLTE aktiviert werden (PPL, Protected Mode Light). Die Speicherung der LAN-Manager-Hashwerte bei Kennwortänderungen SOLLTE per Gruppenrichtlinie deaktiviert werden. Die Überwachungseinstellungen SOLLTEN gemeinsam mit den Serverkomponenten von DirectAccess sorgfältig auf die Anforderungen des Informationsverbunds abgestimmt werden. Es SOLLTE eine Protokollierung auf Clientseite sichergestellt werden.

SYS.2.2.2.A13 Anbindung von Windows 8.1 an den Microsoft Store (S)

Die Möglichkeit, Apps aus dem Microsoft Store zu installieren, SOLLTE deaktiviert werden, sofern sie nicht benötigt wird.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.2.2.2 *Clients unter Windows 8.1* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

SYS.2.2.2.A14 Anwendungssteuerung mit Software Restriction Policies und AppLocker (H)

Anwendungen in Pfaden, in denen Benutzer Schreibrechte haben, SOLLTEN durch Software Restriction Policies (SRP) oder AppLocker an der Ausführung gehindert werden. AppLocker- und SRP-GPO in einem domänenbasierten Netz SOLLTEN NUR zentralisiert mittels Gruppenrichtlinienobjekten je Benutzer bzw. Benutzergruppe verwaltet werden.

AppLocker SOLLTE nach dem Ansatz einer Positivliste (Whitelist) genutzt werden. Alle Anwendungen, die nicht explizit erlaubt sind, SOLLTEN verboten werden. Es SOLLTEN bevorzugt Regeln auf der Grundlage von Anwendungssignaturen definierter Herausgeber genutzt werden. Versuchte

Regelverstöße SOLLTEN protokolliert und geeignet ausgewertet werden.

Für Clients mit besonders hohen Sicherheitsanforderungen SOLLTE AppLocker die Ausführung aller ungenehmigten Anwendungen verhindern, statt diese zu protokollieren.

Die Umsetzung der SRP- und AppLocker-Regeln SOLLTE vor dem Einsatz auf einem produktiven System zunächst auf einem Testsystem oder durch den Betrieb im Überwachungsmodus erprobt werden.

SYS.2.2.2.A15 Verschlüsselung des Dateisystems mit EFS (H)

Bei erhöhtem Schutzbedarf SOLLTE das Dateisystem verschlüsselt werden. Wird hierzu das Encrypting File System (EFS) verwendet, SOLLTE ein komplexes Passwort für den Schutz der mit EFS verschlüsselten Daten verwendet werden. Zusätzlich SOLLTEN die mit EFS verschlüsselten Dateien durch restriktive Zugriffsrechte geschützt werden. Der Wiederherstellungsagent SOLLTE ein dediziertes Konto und nicht das Administratorkonto sein. Der private Schlüssel dieses Kontos SOLLTE auf einen externen Datenträger ausgelagert und sicher aufbewahrt sowie aus dem System entfernt werden. Dabei SOLLTEN von allen privaten Schlüsseln Datensicherungen erstellt werden. Beim Einsatz von EFS mit lokalen Benutzerkonten SOLLTE die Registry mittels Syskey verschlüsselt werden. Die Benutzer SOLLTEN im korrekten Umgang mit EFS geschult werden.

SYS.2.2.2.A16 Verwendung der Windows PowerShell (H)

Wenn die Windows PowerShell (WPS) nicht benötigt wird, SOLLTE sie deinstalliert werden. Es SOLLTE berücksichtigt werden, dass bei Windows 8.1 sich die PowerShell-Skriptumgebung allerdings nur noch dann entfernen lässt, wenn auch das .NET-Framework deinstalliert wird. Daher SOLLTE alternativ die Ausführung der WPS-Dateien nur den Administratoren (lokal und Domäne) gestattet werden. Die Protokollierung von Schreib- und Lesezugriffen auf das Windows PowerShell-Profil SOLLTE aktiviert und die Protokolle regelmäßig kontrolliert werden. Die Ausführung von Windows-PowerShell-Skripten SOLLTE mit dem Befehl *Set-ExecutionPolicy AllSigned* eingeschränkt werden, um zumindest die versehentliche Ausführung unsignierter Skripte zu verhindern.

SYS.2.2.2.A17 Sicherer Einsatz des Wartungscenters (H)

In der Sicherheitsrichtlinie SOLLTE definiert werden, wie die Benutzer mit dem Wartungscenter umgehen sollen. Die Einstellungen für „Neueste Problembehandlungen vom Windows-Onlinedienst für Problembehandlung abrufen“, „Problemberichte senden“, „Regelmäßig Daten über Computerkonfiguration an Microsoft senden“, „Windows-Sicherung“, „Programm zur Benutzerfreundlichkeit“ und „Problembehandlung – andere Einstellungen“ SOLLTEN unter Windows 8.1 deaktiviert werden.

SYS.2.2.2.A18 Aktivierung des Last-Access-Zeitstempels (H)

Wird ein Sicherheitskonzept für ein IT-System mit Windows 8.1 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.2.2.2.A19 Verwendung der Anmeldeinformationsverwaltung (H)

Die Erlaubnis oder das Verbot, Zugangsdaten im sogenannten „Tresor“ zu speichern, SOLLTE in einer Richtlinie festgelegt werden. Ein Verbot SOLLTE technisch durchgesetzt werden.

SYS.2.2.2.A20 Sicherheit beim Fernzugriff über RDP (H)

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung der Remote-Unterstützung berücksichtigt werden. Die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff SOLLTE durch die Zuweisung entsprechender Benutzerrechte und in der Richtlinie festgelegt werden. Eine Remote-Unterstützung SOLLTE nur nach einer expliziten Einladung über EasyConnect oder auf Grundlage einer Einladungsdatei erfolgen. Wird eine Einladung in einer Datei

gespeichert, SOLLTE die Datei mit einem Kennwort geschützt sein. Der aktuell angemeldete Benutzer SOLLTE dem Aufbau einer Sitzung immer explizit zustimmen müssen. Die maximale Gültigkeit der Einladung SOLLTE in der Dauer angemessen sein. Zudem SOLLTE eine starke Verschlüsselung (128 Bit, Einstellung „Höchste Stufe“) verwendet werden. Außerdem SOLLTE die automatische Kennwortanmeldung deaktiviert werden. Es SOLLTE geprüft werden, ob Umleitungen der Zwischenablage, Drucker, Dateiablage und Smartcard-Anschlüsse notwendig sind. Andernfalls SOLLTEN diese deaktiviert werden. Sofern keine Fernsteuerungsmechanismen eingesetzt werden, SOLLTEN diese vollständig deaktiviert werden.

SYS.2.2.2.A21 Einsatz von File und Registry Virtualization (H)

Es SOLLTE geprüft werden, ob der Betrieb von Altanwendungen, die Schreibrechte auf kritische System-Ordner oder Registry-Schlüssel erfordern oder mit Administratorrechten ausgeführt werden müssen, noch notwendig ist. Trifft dies zu, SOLLTE eine Strategie entwickelt werden, um die noch benötigten Altanwendungen durch sichere Alternativen zu ersetzten. Bis zur Ablösung der Altanwendungen SOLLTE geprüft werden, ob zur Absicherung die Windows-Techniken „File Virtualization“ und „Registry Virtualization“ eingesetzt werden können. Die Registry Virtualization SOLLTE nur auf die notwendigen Registry-Schlüssel zugreifen können.

4 Weiterführende Informationen

4.1 Wissenswertes

Der Hersteller Microsoft stellt u. a. folgende weiterführende Informationen zu Windows 8.1 bereit:

- Secure Windows (für Windows 8/8.1, gilt größtenteils auch für Windows Server 2012 / 2012 R2): https://technet.microsoft.com/en-us/library/hh832031.aspx
- Security and Protection: https://technet.microsoft.com/en-us/library/hh831778.aspx
- Security Auditing Overview: https://technet.microsoft.com/en-us/library/dn319078.aspx
- Liste von Sicherheitsereignissen unter Windows 8.1 und Windows Server 2012: https://www.microsoft.com/en-us/download/confirmation.aspx?id=50034
- Konfigurieren von zusätzlichem LSA-Schutz: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein SYS.2.2.2 *Clients unter Windows 8.1* von Bedeutung.

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

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 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen