



SYS.2: Desktop-Systeme

SYS.2.4: Clients unter macOS

1 Beschreibung

1.1 Einleitung

macOS ist ein Client-Betriebssystem der Firma Apple. macOS basiert auf Darwin, dem frei verfügbaren Unix-Betriebssystem von Apple, das wiederum auf dem Open-Source-Betriebssystem FreeBSD aufbaut. macOS setzt sich im Wesentlichen aus Darwin sowie der proprietären grafischen Bedienoberfläche „Aqua“ und weiteren Anwendungen und Diensten zusammen. Gemäß den Lizenzbedingungen von Apple darf macOS nur auf IT-Systemen („Macs“) von Apple installiert werden. Aus diesem Grund sind Eigenheiten dieser Systeme ebenfalls Bestandteil dieses Bausteins.

1.2 Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen, die auf IT-Systemen unter macOS verarbeitet oder mit diesen übertragen werden. Dazu müssen IT-Systeme unter macOS angemessen abgesichert werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.2.4 *Clients unter macOS* ist für alle Client-Systeme anzuwenden, auf denen das Betriebssystem Apple macOS eingesetzt wird.

Der Schwerpunkt liegt in diesem Baustein auf der Absicherung eines Macs mit macOS, der als Stand-alone-System oder als Client in einem Client-Server-Netz betrieben wird. Damit ergänzt der Baustein die allgemeinen Aspekte aus dem zusätzlich anzuwendenden Baustein SYS.2.1 *Allgemeiner Client*. Ein möglicher Einsatz von macOS als Server-Betriebssystem wird im Baustein nicht betrachtet. Im professionellen Einsatz besteht mit dem sogenannten Profilmanager und Mobile Device Management die Möglichkeit, die verwendeten Macs zentral zu verwalten. Diese Lösungen bieten erweiterte Konfigurations- und Verwaltungsfunktionen, werden in diesem Baustein jedoch nicht betrachtet. Entsprechende Sicherheitsaspekte werden im Baustein SYS.3.2.2 *Mobile Device Management (MDM)* behandelt. Außerdem ist zu beachten, dass die beiden Apple-Betriebssysteme macOS (für Macs) und iOS (für iPhones) bzw. iPadOS (für iPads) eng miteinander verzahnt sind. Daher sollte zusätzlich der Baustein SYS.3.2.3 *iOS (for Enterprise)* berücksichtigt werden, wenn neben macOS auch Geräte mit iOS oder iPadOS eingesetzt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.2.4 *Clients unter macOS* von besonderer Bedeutung:

2.1 Unkontrollierbarer Zugriff auf ausgelagerte Daten

macOS bietet eine Reihe von Funktionen, die auf zentralen, von Apple betriebenen Servern ausgeführt werden. Beispielsweise kann Apples iCloud für die Speicherung und für die Synchronisierung von Daten zwischen verschiedenen macOS- und iOS-Geräten verwendet werden. Da hierbei Daten auf Servern Dritter zwischengespeichert werden und damit nicht mehr unter der eigenen Kontrolle stehen, könnten prinzipiell auch Unbefugte auf diese Server zugreifen und die dort gespeicherten oder übertragenen Daten einsehen und für ihre Zwecke missbrauchen.

2.2 Missbrauch der Apple-ID als zentrale Zugangsinformation für Apple-Dienste

Für die Nutzung einiger macOS-Funktionen wird eine eindeutige Apple-ID als Zugangsinformation benötigt. Mit der Apple-ID kann zentral auf verschiedene Apple-Dienste zugegriffen werden, wie beispielsweise auf iCloud, iMessage und den App Store. Falls Unbefugte an die Zugangsinformationen der Apple-ID gelangen, können sie diese Dienste unter Umständen unter einer falschen Identität nutzen und auf Informationen in iCloud zugreifen.

2.3 Angriffe auf Funkschnittstellen

Ein Mac verfügt in der Regel über drahtlose Schnittstellen wie WLAN oder Bluetooth, die zudem von vielen Diensten genutzt werden und entsprechend aktiviert sind. Beispielsweise können mit der WLAN-Funktion Dateien unmittelbar zwischen Apple-Geräten ausgetauscht werden (AirDrop). Des Weiteren kann die WLAN- und Bluetooth-Funktion genutzt werden, um macOS- und iOS-Geräte zu synchronisieren (Continuity). Mit AirPlay ist es möglich, Video- und Audiodaten an kompatible Wiedergabegeräte zu senden. Angreifer könnten versuchen, diese Funkschnittstellen für Angriffe zu missbrauchen, um vertrauliche Informationen zwischen Mac, iPhone, iPad und anderen Geräten abzufangen oder die Geräte zu kompromittieren.

2.4 Angriffe auf Anwendungen mit Vorschau-Funktion

Einige der in macOS integrierten Anwendungen unterstützen eine Vorschaufunktion für bestimmte Dateiformate (z. B. Bilddateien). Dazu gehören der Finder, der Browser „Safari“ und das in macOS integrierte E-Mail-Programm. Die Vorschaufunktion stellt beispielsweise automatisch den Anhang einer E-Mail auszugsweise dar, wenn das Dateiformat bekannt ist. Ein Angreifer könnte somit versuchen, Schadcode im Anhang einer E-Mail zu verstecken. Die Vorschaufunktion würde den E-Mail-Anhang anzeigen und möglicherweise den Schadcode ausführen, der wiederum den Mac kompromittieren könnte.

2.5 Unsichere Protokolle in macOS oder macOS-Anwendungen

macOS und seine Anwendungen unterstützen verschiedene, zum Teil Apple-eigene Protokolle (z. B. AFP) zur Kommunikation mit zentralen Servern oder anderen Endgeräten. Wenn diese Kommunikationsprotokolle keine ausreichenden Sicherheitsmechanismen aufweisen oder unsicher konfiguriert werden, könnten die darüber übertragenen Daten unerlaubt mitgelesen, verfälscht oder anderweitig missbraucht werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.4 *Clients unter macOS* 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.2.4 *Clients unter macOS* vorrangig erfüllt werden:

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

Die Einführung von macOS MUSS sorgfältig geplant werden. Es MUSS entschieden werden, wo und wie Daten abgelegt werden. Es MUSS geplant werden, wie die Datensicherung in das institutionsweite Datensicherungskonzept integriert werden kann. Es MUSS geplant werden, wie Sicherheits- und sonstige Aktualisierungen für macOS und Anwendungen systematisch installiert werden können. Es MUSS ermittelt werden, welche Anwendungen bei einem Plattformwechsel zu macOS benötigt werden. Wird der Mac in einem Datennetz betrieben, MUSS zusätzlich berücksichtigt werden, welche Netzprotokolle eingesetzt werden sollen.

SYS.2.4.A2 Nutzung der integrierten Sicherheitsfunktionen von macOS (B)

Die in macOS integrierten Schutzmechanismen „System Integrity Protection“ (SIP), „Xprotect“ und „Gatekeeper“ MÜSSEN aktiviert sein. Gatekeeper DARF NUR die Ausführung signierter Programme erlauben, sofern unsignierte Programme nicht zwingend notwendig sind.

SYS.2.4.A3 Verwendung geeigneter Benutzerkonten [Benutzer] (B)

Das bei der Erstkonfiguration von macOS angelegte Administrator-Konto DARF NUR zu administrativen Zwecken verwendet werden. Für die normale Verwendung des Macs MUSS ein Standard-Benutzerkonto angelegt werden. Sollte der Mac von mehreren Benutzern verwendet werden, MUSS für jeden Benutzer ein eigenes Konto angelegt werden. Das Gast-Benutzerkonto MUSS deaktiviert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.2.4 *Clients unter macOS*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.4.A4 Verwendung einer Festplattenverschlüsselung (S)

Festplatten SOLLTEN, insbesondere bei mobilen Macs (z. B. MacBooks), verschlüsselt werden. Wird dazu die in macOS integrierte Funktion FileVault verwendet, DARF das Schlüsselmaterial NICHT online bei Apple gespeichert werden. Der von FileVault erzeugte Wiederherstellungsschlüssel MUSS an einem sicheren Ort aufbewahrt werden. Es SOLLTE geprüft werden, ob ein institutioneller Wiederherstellungsschlüssel für FileVault verwendet werden soll.

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

Die in macOS integrierten Ortungsdienste SOLLTEN deaktiviert werden. Heruntergeladene Daten SOLLTEN NICHT automatisch geöffnet werden. Inhalte von optischen und anderen Medien SOLLTEN NICHT automatisch ausgeführt werden.

SYS.2.4.A6 Verwendung aktueller Mac-Hardware (S)

Werden neue Macs beschafft, SOLLTEN aktuelle Modelle ausgewählt werden. Werden bereits vorhandene Macs eingesetzt, SOLLTE regelmäßig überprüft werden, ob diese sowie das darauf installierte Betriebssystem weiterhin von Apple mit Sicherheits-Updates versorgt werden. Werden die Macs nicht mehr durch Apple unterstützt, SOLLTEN sie nicht mehr verwendet werden.

SYS.2.4.A7 Zwei-Faktor-Authentisierung für Apple-ID [Benutzer] (S)

Die Zwei-Faktor-Authentisierung für die Verwendung des Apple-ID-Kontos SOLLTE aktiviert werden.

SYS.2.4.A8 Keine Nutzung von iCloud für schützenswerte Daten [Benutzer] (S)

Es SOLLTE verhindert werden, dass schützenswerte Daten zwischen mehreren Geräten über iCloud-Dienste synchronisiert werden. Stattdessen SOLLTEN Daten nur über selbst betriebene Dienste synchronisiert werden. Schützenswerte Daten SOLLTEN NICHT in iCloud gespeichert werden. Entwürfe, beispielsweise von E-Mails oder Dokumenten, SOLLTEN NICHT automatisch in iCloud gespeichert werden.

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

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

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

Die in macOS integrierte Personal Firewall SOLLTE aktiviert und geeignet konfiguriert werden.

SYS.2.4.A11 Geräteaussonderung von Macs (S)

Bei einer Aussonderung des Macs SOLLTEN der nichtflüchtige Datenspeicher NVRAM (Non Volatile Random Access Memory) sowie der SMC (System Management Controller) zurückgesetzt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.2.4 *Clients unter macOS* 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.2.4.A12 Firmware-Kennwort und Boot-Schutz auf Macs [Benutzer] (H)

Auf älteren Macs SOLLTE die Abfrage eines sicheren Firmware-Kennworts im sogenannten „Command-Modus“ aktiviert werden, um ein unberechtigtes Booten des Macs von einem anderen Startlaufwerk zu verhindern. Es SOLLTE geprüft werden, ob über den „Full-Modus“ ein Kennwort bei jedem Startvorgang abgefragt werden sollte.

Auf Macs mit T2-Sicherheitschip SOLLTE ein Firmware-Passwort über das Start sicherheitsdienstprogramm gesetzt werden. Die Option „Sicheres Starten: Volle Sicherheit“ SOLLTE aktiviert werden. Die Option „Starten von externen Medien nicht zulassen“ SOLLTE aktiviert werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das National Institute of Standards and Technology (NIST) stellt das Dokument „SP 800-179 Rev. 1 (DRAFT): Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist“ (Oktober 2018) zur Verfügung.

5 Anlage: Kreuzreferenztafel zu elementaren Gefährdungen

Die Kreuzreferenztafel 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.2.4 *Clients unter macOS* von Bedeutung.

- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.21 Manipulation von Hard- oder Software
- 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 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.39 Schadprogramme
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen