Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein SYS.2.4 Clients unter macOS

1. Einleitung

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

Die Sicherheit eines Betriebssystems spielt eine wichtige Rolle für die Sicherheit in einem Informationsverbund. Schwachstellen auf der Betriebssystemebene können die Sicherheit aller Anwendungen und aller IT-Systeme des gesamten Netzes beeinträchtigen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.2.4 *Clients unter macOS* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1 Maßnahmen zum Baustein SYS.2.4 Clients unter macOS

SYS.2.4.M1 Planung des sicheren Einsatzes von macOS (B)

Die geregelte und sichere Einführung von macOS setzt eine umfangreiche Planung voraus. In dieser Maßnahme wird auf softwaretechnische Aspekte eingegangen, um eine reibungslose Projektumsetzung zu ermöglichen. Die verwendeten Hardwarekomponenten in einem macOS-System sind von Apple vorgegeben.

Einführung sowie Plattformwechsel
Bei einem Plattformwechsel von einem anderen Betriebssystem zu macOS muss im Vorfeld geprüft werden, ob gleiche oder gleichwertige Anwendungen für macOS zur Verfügung stehen und ob diese zu bestehenden Systemen kompatibel sind. Dies betrifft nicht nur die Anwendungen, die direkt auf dem Client betrieben werden, sondern auch serverbasierte Anwendungen mit bestimmten Voraussetzungen. Zum Beispiel benötigen bestimmte webbasierte Anwendungen Technologien (z. B. ActiveX, Java), die unter macOS möglicherweise nicht oder nur eingeschränkt Verfügung stehen. Vorhandene Software, die nicht kompatibel zu macOS ist, kann beispielsweise mithilfe einer Software-Virtualisierungslösung betrieben werden. Jedoch ist dies nur als Notlösung anzusehen, da erhöhte Ansprüche an die Hardware gestellt werden und es um ein Vielfaches komplexer ist, eine Anwendung in einer virtualisierten Umgebung zu betreiben.

Generell muss geprüft werden, ob bestehende Software-Lizenzverträge auch macOS-Systeme abdecken. Falls nicht, muss in zukünftigen Lizenzverträgen darauf geachtet werden, dass Software gewählt wird, die auf verschiedenen Plattformen betrieben werden kann bzw. deren Lizenzverträge den Einsatz auf anderen Plattformen gestatten.

Bei der Einführung von macOS-Systemen muss ebenfalls geprüft werden, ob bestehende externe Hardware, wie zum Beispiel Drucker, Kartenlesegeräte oder sonstige benötigte Geräte kompatibel zu macOS sind und entsprechende Gerätetreiber zur Verfügung stehen. Ebenfalls muss geprüft werden, ob die eingesetzten Netzprotokolle von macOS unterstützt werden, um eine Verbindung zwischen unterschiedlichen Systemen herstellen zu können. Wird zum Beispiel das "Andrew File System"-Protokoll (AFS) als verteiltes Netz-Dateisystem verwendet, muss im Vorfeld ein geeigneter Client für macOS gewählt werden.

Benutzerkonzept
Im Vorfeld der Einführung von macOS ist ein Benutzerkonzept zu erstellen, falls es noch nicht vorhanden ist. Es legt fest, mit welchen Rechten die Benutzer bestimmte Arbeiten verrichten können. Bei der Planung des Benutzerkonzepts ist zwischen lokalen und domänenweiten Benutzerkonten zu unterscheiden. Sowohl bei lokalen als auch bei domänenweiten Benutzerkonten ist darauf zu achten, dass die Benutzerrechte möglichst restriktiv gewählt werden. So wird das mögliche Schadensmaß bei einer absichtlichen oder versehentlichen missbräuchlichen Nutzung des Benutzerkontos begrenzt. Unter macOS ist für jeden Benutzer ein Konto mit Standardbenutzer-Rechten einzurichten, das zum täglichen Arbeiten verwendet werden muss.

Wenn die Clients unter macOS in einen Verzeichnisdienst integriert werden, muss der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* beachtet werden. Falls es sich um ein heterogenes Netz mit einem Windows-Server als Basis des Verzeichnisdienstes handelt, ist auch der Baustein APP.2.2 *Active Directory* zu beachten.

Administrationskonzept
Im Vorfeld der Einführung von macOS ist ein Administrationskonzept zu erstellen, falls es noch nicht vorhanden ist. Es sind grundsätzlich zwei verschiedene Konten für die Administration vorgesehen.

macOS unterscheidet zwischen Benutzer- und Administratorenkonten. Ein Benutzer, der unter einem Benutzerkonto angemeldet ist, kann keine Systemeinstellungen verändern, Applikationen in allgemein zugängliche Verzeichnisse installieren oder andere Benutzerkonten verwalten. Administratoren haben hingegen diese genannten Möglichkeiten. Soweit möglich, müssen die Administratoren für ihre Arbeit ein Konto mit den Privilegien eines Standardbenutzers verwenden. Nur wenn diese Privilegien nicht mehr ausreichend sind, kann ein Konto mit administrativen Privilegien genutzt werden. Bei macOS sind Aufgaben, die die erweiterten Rechte eines Administrators erfordern, durch das Symbol eines kleinen Vorhängeschlosses gekennzeichnet. Bei Klick auf das Schloss werden die Zugangsdaten des Administrators abgefragt, danach sind Änderungen mit administrativen Privilegien möglich. Nach der Erfüllung der Aufgaben muss sich der Administrator durch einen weiteren Klick auf das Symbol wieder vom Konto mit administrativen Privilegien abmelden und mit dem Standardbenutzerkonto weiterarbeiten.

Als Besonderheit existiert bei macOS zudem ein root-Konto, das in der Standardeinstellung deaktiviert ist. Außerdem ist für das root-Konto standardmäßig kein Passwort gesetzt. Administratoren- und root-Konto unterscheiden sich dahingehend, dass ein Administratorkonto keine Berechtigung besitzt, um Informationen aus wichtigen Systemordnern zu löschen. Somit kann ein Administrator zwar viele Änderungen am System vornehmen, aber nicht das gesamte Betriebssystem komplett unbrauchbar machen. Es ist jedoch möglich, mit einem Administratorenkonto das root-Konto zu aktivieren und zu nutzen. Die

Deaktivierung des root-Kontos stellt also nur einen unvollständigen Schutz gegen das unbeabsichtigte Löschen von Systemdateien dar. In der Standard-Konfiguration verhindert macOS durch die sogenannte System Integrity Protection (SIP) jedoch einen tiefgehenden Zugriff durch das root-Konto. Aufgrund von Sicherheitsproblemen in der Vergangenheit (vgl. CVE-2017-13872) ist es zusätzlich empfehlenswert, für das root-Konto ein sicheres Passwort festzulegen, auch wenn es nicht verwendet werden bzw. deaktiviert bleiben soll.

Protokollierungskonzept
Um Angriffe oder Unregelmäßigkeiten erkennen zu können, müssen die Protokollierungsmöglichkeiten des einzelnen Systems aktiviert und benutzt werden. Um sinnvoll zu protokollieren, muss im Vorfeld überlegt werden, welche Programme auf dem Client unter macOS eine bedeutende Rolle einnehmen. Allen geschäftskritischen Anwendungen muss ein möglichst hohes Log-Level zugeordnet werden, dadurch können insbesondere alle (Warn-) Meldungen protokolliert werden. In einem Störfall stehen dann genug Informationen zur Fehlerbeseitigung zur Verfügung. Wird ein Client zum Beispiel hauptsächlich zum Versenden von E-Mail-Nachrichten verwendet, sollten jegliche Hinweise bezüglich des E-Mail-Programms an eine zentrale Stelle weitergeleitet und ausgewertet werden. Grundsätzlich sollte der Baustein OPS.1.1.5 *Protokollierung* berücksichtigt werden.

Datenablage, Datensicherung und Verschlüsselung
Es ist festzulegen, wo die Benutzerdaten gespeichert werden. Werden alle relevanten Daten auf Servern gespeichert, so kann auf eine lokale Datensicherung verzichtet werden. Im Gegensatz dazu müssen Datensicherungen zentral durchgeführt werden. Dieses Vorgehen ist jedoch stark von den lokalen Gegebenheiten abhängig. Wird zum Beispiel auf einem Client spezielle Software eingesetzt, die nach einem Defekt nur mit hohem Arbeitsaufwand wieder in Betrieb genommen werden kann, muss eine Datensicherung des Clients in regelmäßigen Zyklen erfolgen. Weitere Informationen zum Thema Datensicherung finden sich im Baustein CON.3 *Datensicherungskonzept*.

Werden mobile Macs eingesetzt, müssen (temporär) die Informationen oft lokal abgelegt werden. Somit muss die clientseitige Datenablage und ihr (kryptographischer) Schutz geplant werden.

Grundsätzlich sollte die gesamte Festplatte eines Macs verschlüsselt werden.

Sicherheitsrichtlinie
Eine der wichtigsten organisatorischen Aufgaben bei der Einführung von macOS ist es, eine entsprechende Sicherheitsrichtlinie für macOS zu planen und zu definieren. Diese Richtlinie legt die später umzusetzenden Sicherheitsbestimmungen für macOS Clients fest. Die Sicherheitsrichtlinie muss allen Anwendern und anderen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die in der macOS-Sicherheitsrichtlinie definierten Anforderungen werden durch die entsprechenden Sicherheitseinstellungen auf Betriebssystemebene umgesetzt. In Fällen, in denen technische Maßnahmen nicht ausreichen, müssen sie durch zusätzliche organisatorische Maßnahmen begleitet und unterstützt werden. Nach Möglichkeit kann eine technische Lösung gegenüber einer organisatorischen vorgezogen werden

Die zu erstellende Sicherheitsrichtlinie hat sich an den bisher geltenden Sicherheitsrichtlinien der jeweiligen Institution zu orientieren und darf diesen nicht widersprechen. In der Regel werden die existierenden Regelungen für macOS angepasst oder sinngemäß erweitert. Dabei sind insbesondere spezifische Funktionen von macOS wie beispielsweise FileVault und Time Machine zu berücksichtigen. Generell gilt, dass sich die Planung der macOS-Infrastruktur an der jeweiligen übergreifenden Sicherheitsrichtlinie orientiert. Die Infrastruktur beeinflusst jedoch über einen Feedback-Prozess diese übergreifende Sicherheitsrichtlinie. Nicht zuletzt ist beim Erstellen der Sicherheitsrichtlinie darauf zu achten, dass geltende rechtliche Bestimmungen berücksichtigt werden. Die Sicherheitsrichtlinie für macOS ist zu dokumentieren und den Benutzern des Client-Server-Netzes im erforderlichen Umfang mitzuteilen. Alle Administratoren müssen die Sicherheitsrichtlinie kennen und umsetzen.

Datensicherung und Wiederherstellung von macOS Clients
Damit Daten im Bedarfsfall wiederhergestellt werden können, müssen regelmäßige Backups angelegt werden. Darüber hinaus muss jedes angelegte Backup verschlüsselt werden. Hierzu kann die in macOS integrierte Funktion "Time Machine" oder eine Drittanbieterlösung verwendet werden.

"Time Machine" steht bereits bei einer Standardinstallation von macOS zur Verfügung. Time Machine lässt sich auch von den Benutzern leicht konfigurieren, mit dem Programm können vollständige Festplatten gesichert werden.

Im ersten Schritt erzeugt Time Machine eine vollständige Kopie der zu sichernden Informationen, anschließend werden nur noch Informationen gesichert, die seit der letzten Datensicherung verändert wurden oder neu hinzugekommen sind (inkrementelle Datensicherung).

Werden die Informationen mit Time Machine gesichert, sollten folgende Punkte beachtet werden:

- Die Daten auf den Sicherungsmedien sind standardmäßig unverschlüsselt. Das Backup muss daher verschlüsselt oder vor unbefugtem Zugriff geschützt aufbewahrt werden.
- Die gesicherten Informationen werden nicht komprimiert und können mehr als den eingeplanten Speicherplatz belegen.
- Eine vollständige Wiederherstellung der gespeicherten Daten kann zeitintensiv sein.
- Die Datensicherung erfolgt automatisch alle 30 Minuten nach dem Start des IT-Systems. Allerdings können Benutzer ein Backup manuell zu jedem Zeitpunkt auslösen.
- Es können bei einer Sicherung über ein Datennetz ohne zusätzliche Systemeingriffe nur spezielle Network-Attached-Storage-Systeme (NAS) genutzt werden.

Aufgrund dieser und weiterer limitierender Faktoren ist der Einsatz von Time Machine prinzipiell nur beschränkt zu empfehlen und stark abhängig von den lokalen Gegebenheiten. Bei der Wahl einer Datensicherungssoftware in heterogenen Umgebungen wird empfohlen, ein Programm zur Datensicherung einzusetzen, das mehrere Plattformen wie macOS, Windows und Linux unterstützt.

Mit Time Machine können Datensicherungen auf externen Datenträgern, anderen macOS Systemen oder auf einem internen Datenträger, von dem das System nicht gestartet wurde, abgelegt werden. Sollen lokal angeschlossene Datenträger zur Datensicherung genutzt werden, müssen diese mit dem Dateisystem "Mac OS Extended (Journaled)" formatiert sein. Alternativ kann eine Datensicherung in einem freigegebenen Verzeichnis auf einem entfernten System im Netz abgelegt werden. Voraussetzung hierfür ist die Nutzung des Apple Filing Protocols (AFP). Das SMB / CIFS -Protokoll kann mit folgendem Befehl auf der Konsole aktiviert werden:

defaults write com.apple.systempreferences TMShowUnsupportedNetworkVolumes 1

Die Variable "TMShowUnsupportedNetworkVolumes" ist ein inoffizieller Weg, um weitere Netzwerkprotokolle freizuschalten. Damit kann aber kein fehlerfreier Einsatz garantiert werden und Apple gewährt auch keine Unterstützung für dieses Vorgehen.

Time Machine kann in den Systemeinstellungen unter "Time Machine" aktiviert werden. Anschließend muss ein kompatibles Laufwerk zur Ablage der Datensicherung gewählt werden. Time Machine erstellt eine Kopie aller auf der Festplatte befindlichen Daten. Sollen Daten von der Datensicherung nicht erfasst werden, lassen sich Ausnahmen in den Optionen definieren. Reicht der verfügbare Speicherplatz nicht mehr aus, um eine Datensicherung durchzuführen, wird der Anwender darauf aufmerksam gemacht, dass er entweder ältere Datensicherungen löschen muss, oder dass das Programm automatisch ältere Sicherungen löscht, bis genug Speicherplatz zur Verfügung steht.

Bei der Durchführung einer Datensicherung sind die folgenden Punkte zu beachten:

- Time Machine kann alle Systemdateien, die zum Start des lokalen Rechners notwendig sind, sichern. Eine Datensicherung sollte automatisch in regelmäßigen Abständen und manuell nach größeren Änderungen der Konfiguration durchgeführt werden.

- Nach Abschluss der Datensicherung ist die zugehörige Protokolldatei /var/log/system.log daraufhin zu überprüfen, ob während der Sicherung Fehler aufgetreten sind. Die Protokolldatei kann über das macOS-Dienstprogramm "Konsole" eingesehen werden. Die Datensicherung wird vom Prozess "backupd" erstellt, sodass nach allen Meldungen mit diesem Prozessnamen gesucht werden kann. Da in der Protokolldatei /var/log/system.log unter anderem vertrauliche Informationen aufgelistet sind, kann sie nur ein Benutzer mit Administrator-Privilegien einsehen.

Systemwiederherstellung
Um ein komplettes System wiederherzustellen, muss der Client entweder von einem Installationsmedium (DVD oder USB-Stick) oder im Recovery-Modus gestartet werden. Dazu muss während des Startvorganges die Alt-Taste (für USB-Sticks), die Taste C (für optische Medien) oder die Tastenkombination Cmd+R (für Recovery-Modus) gedrückt gehalten werden. Nach Auswahl der Menüsprache findet sich in den Dienstprogrammen die Möglichkeit, eine Datenwiederherstellung durchzuführen. Anschließend müssen der Datenträger, auf der sich die Datensicherung befindet, und die Festplatte, die wiederhergestellt werden soll, ausgewählt werden.

Time Machine kann auch nur ausgewählte Dateien wiederherstellen. Dazu müssen in den verschiedenen, hintereinander dargestellten, zeitlich geordneten Fenstern die Objekte in der gewünschten Version ausgewählt und über die Schaltfläche "Wiederherstellen" zum Zielort kopiert werden.

Anforderung an Sicherungssoftware für macOS
Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, ist bei der Auswahl der Sicherungssoftware darauf zu achten, dass sie so viele der folgenden Anforderungen wie möglich erfüllt:

- Die bei macOS eingesetzten Dateisysteme APFS und HFS+ müssen bei der Sicherung und Wiederherstellung unterstützt werden. Weitere unterstützte Dateisysteme wie FAT und NTFS sind von Vorteil.
- Es muss möglich sein, Sicherungen automatisch zu frei definierbaren Zeiten oder in einstellbaren Intervallen durchführen zu lassen, ohne dass Eingriffe außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern erforderlich wären.
- Die Sicherungssoftware muss den Schutz des Backup-Mediums vor unbefugtem Zugriff durch ein Passwort oder besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Von Vorteil ist es, wenn ein oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen informiert werden können.
- Das Erstellen von Include- und Exclude-Listen muss möglich sein. Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche übersprungen werden können. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe zu benutzen.
- Die Sicherung sollte auf verschiedenen Datenträgern wie optischen Datenträgern, auf Festplatten, Bandlaufwerken, USB-Laufwerken sowie Netzlaufwerken erfolgen können.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung einer Volldatensicherung sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.

- Bei der Wiederherstellung von Dateien sollte ausgewählt werden können, ob die Dateien am ursprünglichen oder an einem anderen Ort wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte einstellbar sein, ob diese Datei immer, nie oder nur in dem Fall überschrieben wird, dass sie älter ist als die zu rekonstruierende Datei, oder dass in diesem Fall eine explizite Anfrage an den Benutzer erfolgt.

Wiederherstellung von Systemparametern beim Einsatz von macOS
Falls ein macOS-System nicht mehr startet oder Probleme mit der Lesbarkeit von Dateien auftreten, gibt es verschiedene Handlungsmöglichkeiten. Benutzer und Administratoren sind über die Maßnahmen zur Wiederherstellung von Systemparametern beim Einsatz von macOS zu informieren. Um Fehler bei der Nutzung eines Clients unter macOS zu finden, die einen normalen Betriebssystem-Start verhindern, kann zwischen verschiedenen Startmodi gewählt werden.

Single-User-Mode
Wird ein Client unter macOS gestartet, muss die Tastenkombination Cmd+S gedrückt gehalten werden, um in den Single-User-Modus zu gelangen. Der Single-User-Modus bootet nur ein rudimentäres Betriebssystem ohne grafische Benutzeroberfläche. Dieser Modus ist sehr robust und meistens auch dann noch verfügbar, wenn das System durch eine fehlgeschlagene Installation oder einen Dateisystemfehler nicht mehr startet. Zur Arbeit im Single-User-Modus wird zwar das root-Konto verwendet, jedoch kann zu Beginn nur mit Leserechten auf das Startlaufwerk zugegriffen werden.

Um das Dateisystem zu überprüfen, kann der Befehl "/sbin/fsck -fy" eingegeben werden. Es ist zu beachten, dass im Single-User-Modus die amerikanische Tastaturbelegung verwendet wird.

Wurde das Dateisystem überprüft und gegebenenfalls repariert, so kann durch den Befehl "/sbin/mount -uw /" der Schreibzugriff auf das Startlaufwerk aktiviert werden. Nun stehen weitere Möglichkeiten zur Verfügung, um den Fehler zu beseitigen. So können beispielsweise fehlerhafte Programme entfernt werden, die automatisch mit dem System starten.

Verbose-Mode
Der "Verbose-Mode" bietet eine weitere Möglichkeit, um tiefere Einblicke in das System zu erhalten. Um in diesen Modus zu kommen, muss während des Systemstarts die Tastenkombination Cmd+V gedrückt gehalten werden. Dadurch wird das System normal gestartet, die Bildschirmausgabe jedoch nicht mehr durch das Apple-Logo verdeckt. Statt dessen zeigt das System Informationen an, die zum Beispiel Auskunft darüber geben, welcher Dienst gerade gestartet wird. So können mögliche Fehlerquellen weiter eingegrenzt werden.

Safe-Boot-Mode
Wird während des Startvorgangs die Taste "Shift" gedrückt gehalten, werden keine Kernel-Extensions und Startobjekte von Fremdherstellern geladen. Somit wird bereits während des Starts eine hohe Zahl an Fehlerquellen ausgeschlossen. Wurde festgestellt, dass eines der Startobjekte den regulären Betriebssystemstart verhindert, kann das entsprechende Startobjekt in den "Systemeinstellungen" unter "Benutzerkonten" deaktiviert werden. Die nicht über die grafische Oberfläche erreichbaren Startobjekte befinden sich im Verzeichnis „/Library/StartupItems/“.

Startobjekte anpassen
Wird durch den Safe-Boot-Mode festgestellt, dass ein Startobjekt Probleme verursacht und die grafische Benutzeroberfläche nicht eingesetzt werden kann, um das Objekt zu entfernen, muss manuell auf die Startobjekte zugegriffen werden. Die Startobjekte des "LaunchDaemons", die mit root-Privilegien ausgeführt werden, befinden sich entweder in den Verzeichnissen "/System/Library/LaunchDaemons" oder "/Library/LaunchDaemons". Startobjekte, die mit Benutzer-Privilegien ausgeführt werden, sind in den Verzeichnissen "/System/Library/LaunchAgents" oder "/Library/LaunchAgents" zu finden. Um ein Startobjekt zu entfernen, reicht es aus, die Dateiendung zu verändern.

Parameterspeicher löschen
Im Permanent Random Access Memory (PRAM) werden Systeminformationen wie die Wiederholfrequenz, Auflösung und Farbtiefe, aber auch Informationen über das Startlaufwerk gespeichert. Um den Parameterspeicher zu löschen, muss beim Starten des Computers die Tastenkombination Command+Alt+P+R gleichzeitig gedrückt gehalten werden, bis der Startton mehrmals zu hören ist.

Power Management Unit zurücksetzen
Startet das System nach einem PRAM-Reset noch immer nicht, sollte die Power Management Unit zurückgesetzt werden. Da sich die Vorgehensweise stark von Produkt zu Produkt unterscheidet, sollte der Anwender die Apple-Wissensdatenbank im Internet zu Rate ziehen.

SYS.2.4.M2 Nutzung der integrierten Sicherheitsfunktionen von macOS (B)

macOS enthält "Xprotect", einen integrierten Schutz gegen bekannte, Mac-spezifische Schadprogramme, der durch Apple in unregelmäßigen Abständen aktualisiert wird und standardmäßig aktiviert ist. Zusätzlich enthält macOS mit dem sogenannten "Gatekeeper" eine Funktion, welche die Ausführung von Anwendungen kontrolliert. Standardmäßig erlaubt Gatekeeper nur die Ausführung von Programmen, die entweder über den App Store bezogen oder von Apple signiert wurden (das Programm stammt von einem Entwickler, der von Apple verifiziert wurde). Die Funktion Gatekeeper muss in dieser Standardkonfiguration betrieben werden, solange unsignierte Programme nicht absolut nötig sind.

Manuelle Überprüfung der Signaturen von macOS Anwendungen
In macOS sind Betriebssystemkomponente sowie Programme aus dem App Store von Apple digital signiert. Darüber hinaus sind Dritthersteller, die ihre Programme nicht im App Store anbieten, aufgerufen, ihre Programme zu signieren. Wird ein signiertes Programm in irgendeiner Form verändert, zum Beispiel durch Schadsoftware, so wird die Signatur ungültig. Wird ein neues Programm eingesetzt, muss daher dessen Signatur manuell überprüft werden. Liegen keine Signaturinformationen vor, sollte das Programm zumindest mit einem Viren-Schutzprogramm überprüft werden. Um die Gültigkeit einer Signatur zu überprüfen, wird von Apple eine Public-Key-Infrastruktur verwendet, ähnlich wie bei HTTPS-Webseiten. Die Administratoren sollten im Umgang mit dem Befehl "codesign" geschult werden, um jedes neue Programm einer einmaligen Signaturprüfung unterziehen zu können. Ob ein Programm eine gültige Signatur hat, kann mit folgendem Kommandozeilen-Befehl überprüft werden:

codesign --verify --verbose /Pfad/Dateiname.app

Handelt es sich um eine gültige Signatur, so entspricht die Datei dem vom Hersteller vertriebenen Original und wurde nicht verändert. Somit kann mit einer Signaturprüfung eine mögliche Manipulation auf dem Übertragungsweg ausgeschlossen werden.

Signaturen werden ebenfalls genutzt, um Programme eindeutig wiederzuerkennen. So ist sichergestellt, dass für diese Programme die entsprechenden Einstellungen in der "Kindersicherung", der Firewall und dem Schlüsselbund gelten.

Einschränkung der Programmzugriffe unter macOS
Um unter macOS den Zugriff auf bestimmte Funktionen des Computers einzuschränken, kann die "Kindersicherung" eingesetzt werden. Obwohl diese Funktion Kindersicherung bezeichnet wird, kann deren Nutzung auch in Behörden oder Unternehmen sinnvoll sein. Durch diese Kindersicherung, zu finden in den Systemeinstellungen, können Benutzerkonten weiter eingeschränkt werden. Auch die Programmzugriffe lassen sich mit der Kindersicherung weiter einschränken, nachdem alle nicht benötigten Programme entfernt wurden. Unter Umständen können Einschränkungen hierdurch präziser eingestellt werden.

So kann zum Beispiel für die Benutzer der Zugriff auf bestimmte Anwendungsprogramme, Webseiten oder Computerkomponenten beschränkt werden. Dieses Vorgehen ist auch geeignet, um das Verzeichnis "Dienstprogramme" zu sperren, da hier Programme zur Administration des Computers liegen, die tiefere Einblicke in das System ermöglichen. Soll nur der Zugriff auf bestimmte Webseiten bzw. Domänen erlaubt sein, kann unter dem Menüpunkt "Inhalt" beziehungsweise "Content" der Zugriff auf eine Domäne wie "*.bund.de" erlaubt werden. Weiterhin ist es möglich, die E-Mail-Kommunikation nur zwischen vorher festgelegten Partnern zu erlauben.

Unter dem Menüpunkt "Mail" kann eine Liste von freigegebenen E-Mail-Kommunikationspartnern erstellt werden. Durch diese Einstellung kann vermieden werden, dass Informationen über das E-Mail-Programm abfließen. Es muss jedoch beachtet werden, dass weiterhin HTTP-Webmailer benutzt werden können, um E-Mails an nicht autorisierte Personen zu versenden. Jedoch ist es zurzeit nicht möglich, die Liste der erlaubten Kommunikationspartner mittels regulären Ausdrücken anzupassen. Die Anmeldezeiten für Benutzerkonten lassen sich unter dem Menüpunkt "Time" anpassen. Wird zum Beispiel davon ausgegangen, dass die Hauptarbeitszeit zwischen 7 und 17 Uhr liegt, sollten die erlaubten Benutzeranmeldezeiten diesen Zeiten ungefähr entsprechen.

Weitere verfügbare Einstellungsmöglichkeiten, wie zum Beispiel der Zugriff auf optische Laufwerke, sollten möglichst restriktiv gehalten werden. Jedoch muss beachtet werden, dass eine zu starke Einschränkung hinderlich und demotivierend sein kann. Daher sollte im Vorfeld durch den Leiter der IT und den ISB geklärt werden, welche Restriktionen an welchen Clients umgesetzt werden sollen. Dies sollte dokumentiert werden.

Die Clients können ebenfalls zentral gesteuert werden. Wird in den "Systemeinstellungen" unter "Kindersicherung" die Option "Kindersicherung von einem anderen Computer aus verwalten" aktiviert, können Benutzerkonten auf entfernten Computern mittels Kindersicherung eingeschränkt werden. Hierfür wird der Benutzername und das Passwort eines Administrators auf dem zu steuernden IT-System benötigt. Mit diesen Zugangsdaten können die Benutzerrechte auf dem zu steuernden IT-System vom administrierenden IT-System aus, so wie oben beschrieben, eingeschränkt werden.

SYS.2.4.M3 Verwendung geeigneter Benutzerkonten (B)

Das bei der Erstkonfiguration von macOS angelegte Benutzerkonto ist ein Administrator-Konto mit umfassenden Berechtigungen zur Systemkonfiguration. Es muss daher für die tägliche Verwendung des Macs auf jeden Fall zusätzlich ein Standard-Benutzerkonto angelegt werden. Sollte der Mac von mehreren Anwendern genutzt werden, muss für jeden Anwender ein eigenes Benutzerkonto angelegt werden. Es sollten nur solche Anwender administrative Aufgaben auf dem System wahrnehmen dürfen, die diese Funktionalität auch benötigen und beherrschen.

Gast-Benutzer-Account deaktivieren
Der Gast-Benutzer-Account unter macOS ist standardmäßig aktiviert und muss zusammen mit dem Zugriff für Gäste auf freigegebene Ordner deaktiviert werden. Unter "Systemeinstellungen | Benutzer | Andere Accounts | Gast-Account" muss die Option "Gästen den Zugriff auf freigegebene Ordner erlauben" deaktiviert werden.

Zugriffsschutz der Benutzerkonten unter macOS
Unter macOS müssen die Einstellungen der Benutzerkonten angepasst werden, um die System-Sicherheit weiter zu erhöhen. Zum Beispiel könnte die Merkhilfe für Passwörter von Unbefugten genutzt werden, um Hinweise auf das Passwort zu erhalten. Diese Anpassungen lassen sich in den Systemeinstellungen unter "Benutzer" vornehmen.

Die Sicherheit eines Benutzerkontos vor unbefugtem Zugriff ist im hohen Maße von dem verwendeten Passwort abhängig, daher muss ein starkes Passwort verwendet werden. Eine weitere wichtige Bedingung für ein sicheres Benutzerkonto ist das Deaktivieren von Merkhilfen des Passwortes, durch die ein Angreifer wichtige Hinweise auf das Passwort erhalten kann. Da die Informationen in der Merkhilfe im schlimmsten Fall dem eigentlichen Passwort entsprechen, sollte diese Funktion deaktiviert werden. Wird eine Passwort-Merkhilfe dennoch eingesetzt, müssen unbedingt alle Benutzer für diese mögliche Gefahr sensibilisiert werden. Ebenfalls sollte das Anmeldefenster nicht in Form einer Liste aller Benutzer angezeigt werden, da ein Angreifer damit alle Informationen über auf dem System existierende Benutzer erhält. Er benötigt dann nur noch die entsprechenden Passwörter, um unerlaubten Zugriff auf das System zu erhalten. Ohnehin sollte die Anmeldung am System grundsätzlich nicht automatisch erfolgen, sondern nur mit Benutzername und Passwort möglich sein.

Festlegung von Passwortrichtlinien unter macOS
Für alle Clients unter macOS müssen Richtlinien für Passwörter definiert werden, um sie mit einem angemessenen starken Passwort zu versehen. Dazu kann das Kommandozeilen-Programm "pwpolicy" benutzt werden. Mit diesem Programm lassen sich beispielsweise eine minimal erforderliche Anzahl von

Buchstaben und Zahlen, eine Mindestzeichenlänge oder eine maximale Anzahl fehlgeschlagener Login-Versuche definieren.

Der folgende Befehl legt eine Richtlinie für Passwörter fest, die eine Minimallänge des Passwortes von 8 Zeichen fordert und 8 fehlgeschlagene Anmeldeversuche zulässt, bevor das Konto deaktiviert wird.

pwpolicy -n /Local/Default -setglobalpolicy "minChars=8 maxFailedLoginAttempts=8"

Automatische Anmeldung deaktivieren
Das automatische Anmelden am System sollte deaktiviert werden. Ist es möglich, sich an einem macOS-System ohne Passwortabfrage anzumelden, werden viele Sicherheitsfunktionen übergangen. Die Option "Automatisches Anmelden deaktivieren" ist in den Systemeinstellungen unter Sicherheit im Menüpunkt "Allgemein" zu finden und sollte aktiviert werden.

Aktivierung der Bildschirmsperre
Wird der Bildschirmschoner oder der Ruhezustand beendet, sollte das Kennwor erneut für den aktuell angemeldeten Benutzer abgefragt werden. Die Option "Kennwort erforderlich" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden und sollte aktiviert werden. Dieser Wert sollte möglichst niedrig gewählt werden. Es empfiehlt sich eine Einstellung von höchstens 15 Minuten.

Abmelden nach x Minuten Inaktivität
Befindet sich das IT-System längere Zeit im Leerlauf, kann eine automatische Abmeldung des Benutzers sinnvoll sein. Die Option "Abmelden nach x Minuten Inaktivität" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden und kann aktiviert werden. Dieser Wert sollte möglichst niedrig gewählt werden. Wenn das System den Benutzer nach einer bestimmten Zeit automatisch abmelden soll, empfiehlt sich eine Einstellung von 15 Minuten.

Sicherheit des Schlüsselbundes erhöhen
Das Passwort des Schlüsselbundes sollte geändert werden, sodass es nicht mehr mit dem Passwort des aktuell angemeldeten Benutzers übereinstimmt. Damit wird verhindert, dass eine Person, die unberechtigten Zugang zum Client erlangt, auch Zugang zu allen Informationen im Schlüsselbund erhält. Um das Passwort zu ändern, muss unter den Dienstprogrammen die Applikation "Schlüsselbund" aufgerufen und unter dem Menüpunkt "Bearbeiten" die Option "Kennwort für Schlüsselbund 'Anmeldung' ändern" gewählt werden. Dadurch wird die Synchronisation zwischen Benutzeraccount-Passwort und Schlüsselbund-Passwort aufgehoben. Zusätzlich sollte die Option "Einstellungen für den Schlüsselbund 'Anmeldung' ändern" aufgerufen werden, um die Optionen "Nach X Minuten Inaktivität schützen" und "Bei Wechsel in Ruhezustand schützen" zu aktivieren. Bei der ersten Option empfiehlt es sich, 15 Minuten einzustellen.

Verwenden der Passwortabfrage für jede Systemeinstellung
Es sollte die "Kennwortabfrage für die Freigabe jeder geschützten Systemeinstellung" aktiviert werden, damit nur Administratoren die Systemeinstellungen ändern können. Weiterhin sorgt diese Einstellung dafür, dass bei einem unbefugten Zugriff nur freigeschaltete Systemeinstellungen verändert werden können. Die Option "Kennwortabfrage für die Freigabe jeder geschützten Systemeinstellung" ist in den Systemeinstellungen unter Sicherheit in dem Menüreiter "Allgemein" zu finden.

Gemeinsam mit den Basis-Maßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich SYS.2.4 *Clients unter macOS*.

SYS.2.4.M4 Verwendung einer Festplattenverschlüsselung (S)

Mit aktivierter Festplattenverschlüsselung sind die Festplatten-Daten eines Macs im ausgeschalteten Zustand verschlüsselt. Die Festplattenverschlüsselung muss daher insbesondere bei mobilen Macs (z.B. MacBooks) verwendet werden. Hierzu kann beispielsweise die in macOS integrierte Funktion "FileVault" verwendet werden.

Mit FileVault können Partitionen mit dem Algorithmus AES-XTS-128 verschlüsselt werden. Da es sehr einfach zu benutzen ist, wird empfohlen, alle Partitionen des Macs generell zu verschlüsseln. Das gilt

besonders für sensible Informationen auf mobilen Rechnern, die einem erhöhten Diebstahlsrisiko ausgesetzt sind.

FileVault schützt die Informationen nur, wenn der Client ordnungsgemäß heruntergefahren wurde oder der Benutzer noch nicht angemeldet ist. Nachdem sich der Benutzer erfolgreich angemeldet hat, wird die von FileVault verschlüsselte Partition in das System eingebunden und ist verfügbar. Meldet sich der Benutzer ab, wird die von FileVault verschlüsselte Partition wieder aus dem Dateisystem ausgehängt und die Dateien sind geschützt.

Können sich die Benutzer ohne Authentisierung am Client anmelden ("Automatische Anmeldung"), werden die mit FileVault geschützten Informationen ohne Passwortabfrage entschlüsselt. Für wirksamen Schutz der Informationen durch FileVault muss die automatische Anmeldung deaktiviert und ein ausreichend sicheres Passwort gewählt werden.

Vorbereitung des Einsatzes von FileVault
Mit FileVault können nur Partitionen geschützt werden, die mit den Dateisystemen HFS+ ("Mac OS Extended") oder APFS formatiert sind und bei denen der Zusatz "Case sensitive" bzw. "Groß- und Kleinschreibung" nicht aktiviert wurde.

FileVault aktivieren
Um das Startvolume eines Macs zu verschlüsseln, kann FileVault in den Systemeinstellungen aktiviert werden. Wenn FileVault auf einem Mac mit mehr als einem Benutzer aktiviert wird, erscheint die Aufforderung, die jeweiligen Benutzer anzugeben, die das Startvolume entsperren können.

Datenwiederherstellung
Beim Aktivieren von FileVault erhält man einen Wiederherstellungsschlüssel, der dazu verwendet werden kann, die Daten auf dem verschlüsselten Startvolume wiederherzustellen, falls der Benutzer das Passwort vergessen sollte. Der Wiederherstellungsschlüssel darf nicht online bei Apple gespeichert werden. Der von FileVault erzeugte Wiederherstellungsschlüssel muss an einem sicheren Ort aufbewahrt werden.

Besteht der Verdacht, dass der Wiederherstellungsschlüssel publik wurde, weil er zum Beispiel an einem ungesicherten Ort aufbewahrt worden ist, muss er sofort geändert werden, da sonst der Zugriff auf alle auf dem Computer befindlichen verschlüsselten Daten möglich ist.

Der Wiederherstellungsschlüssel sollte an einer geeigneten Stelle aufbewahrt werden, damit die Daten in einem Störfall schnell und personalunabhängig durch einen Administrator wiederhergestellt werden können.

Sichere Datenhaltung und sicherer Transport unter macOS
Unter macOS können Disk-Images erstellt werden. Disk-Images stellen sich wie Dateien dar, enthalten jedoch intern ein eigenes Dateisystem, das per Doppelklick als virtuelles Laufwerk in das System eingebunden werden kann. Disk-Images können komprimiert und verschlüsselt werden. Jedes macOS-System kann die so erzeugten Disk-Images problemlos lesen. Auf anderen Plattformen ist dafür zusätzliche Software notwendig. Grundsätzlich sollte darauf geachtet werden, dass vertrauliche Informationen unter macOS nur in einem verschlüsselten Disk-Image oder mittels einer anderen geeigneten Verschlüsselungsmethode transportiert und gelagert werden. Die Benutzer müssen im Umgang mit Disk-Images geschult sein.

Wird ein Disk-Image von einem vorhandenen Verzeichnis erstellt, so werden zwei Einstellungsmöglichkeiten angeboten. Zum einen kann das Image-Format ausgewählt werden, zum Beispiel "Komprimiert", "Nur lesen" oder "Lesen/Schreiben". Für genaue Abbilder von CDs/ DVDs ist das Image-Format "DVD/CD-Master" geeignet. Zum anderen wird eine Verschlüsselung angeboten. Befinden sich vertrauliche Informationen im Disk-Image, sollte es verschlüsselt werden. Hierfür sollte eine 256-Bit- AES - Verschlüsselung sowie ein komplexes Passwort gewählt und triviale Passwörter vermieden werden.

Soll ein neues, leeres Disk-Image erstellt werden, stehen im Gegensatz zu einem Image aus einem vorhandenen Ordner weitere Einstellungsmöglichkeiten zur Verfügung. Als wichtigste Optionen kann die maximale Größe des Disk-Images eingestellt sowie das Image-Format ausgewählt werden. Wird ein

"Mitwachsendes Bundle-Image" gewählt, so wird Festplattenspeicher nur dann belegt, wenn er benötigt wird. Das Image wächst mit den hinzugefügten Daten. Das "Mitwachsende Bundle-Image" schrumpft jedoch nicht, wenn Daten wieder daraus entfernt werden. Belegter Speicher lässt sich jedoch im Nachhinein wieder freigeben. Eine weitere Einstellung bei einem neu erstellen Disk-Image ist die Wahl zwischen den gängigen Dateisystemen von Apple und Microsoft.

Das Kennwort für das Disk-Image kann ebenfalls wie andere vertrauliche Informationen im Schlüsselbund abgelegt werden. Arbeiten mehrere Personen mit einem Disk-Image, muss ein zentraler, sicherer Ablageort gewählt werden, damit das aktuelle Passwort jedem autorisierten Mitarbeiter zur Verfügung steht.

Einsatz von Apple-Software-Restore unter macOS
Unter macOS können Dateisysteme mit der Funktion Apple-Software-Restore (ASR) dupliziert und geklont werden. ASR bietet nicht nur die Möglichkeit, Partitionen zu klonen, sondern auch ein Disk-Image im Netz bereitzustellen und dieses über das Netz auf Clients zu verteilen.

Wurde ein Client unter macOS nach den Vorgaben des Unternehmens oder der Behörde installiert und entspricht den Sicherheitsrichtlinien, so kann dieses System geklont und für eine Netz-Installation für weitere Clients genutzt werden. Damit wird es ermöglicht, dass alle Clients unter macOS eine gleiche Grundkonfiguration erhalten, die den Sicherheitsvorgaben der Institution entspricht.

SYS.2.4.M5 Deaktivierung sicherheitskritischer Funktionen von macOS (S)

macOS bietet verschiedene Funktionen, um dem Benutzer einen hohen Bedienkomfort zu ermöglichen. Dazu gehören beispielsweise die Ortungsdienste, das Speichern zuletzt verwendeter Objekte, das automatische Öffnen von heruntergeladenen Daten und das automatische Starten von CDs und DVDs. Da diese Funktionen allerdings einen negativen Einfluss auf den Datenschutz des Benutzers haben, sollten diese Funktionen deaktiviert bzw. konfiguriert werden.

Ortungsdienste deaktivieren
Unter Verwendung der Daten aus WLAN-Netzen ist es möglich, den ungefähren Aufenthaltsort eines macOS Clients zu ermitteln. Diese Standortinformationen können dazu verwendet werden, Systemdienste wie die Zeitzone für das aktuelle Datum und die Uhrzeit automatisch einzustellen. Jedoch können auch Webseiten mit Lokalisierungsfunktion diese Informationen nutzen, um den Standort des Webseiten-Besuchers zu bestimmen. Dies kann nützlich, aber auch aus Datenschutz- und Sicherheitssicht problematisch sein. Beispielsweise kann mithilfe der Ortungsdienste der Standort des nächsten Bankautomaten oder Postamtes angezeigt werden. Möchte eine Webseite den Standort lokalisieren, erscheint normalerweise ein Dialogfenster, um die Erlaubnis des Benutzers dazu einzuholen. Dennoch sollten die Ortungsdienste in den Systemeinstellungen generell deaktiviert werden.

Automatisches Öffnen "sicherer Dateien" in Safari deaktivieren
Der mitgelieferte Browser Safari bietet die Möglichkeit, Dateien direkt nach einem Download mit dem damit verknüpften Programm zu öffnen. Diese Einstellung ermöglicht es auch, Dateien automatisch und ohne Nachfrage auszuführen, die Schadcode enthalten könnten. Wird zum Beispiel aus einer unsicheren Quelle, wie einer manipulierten Webseite im Internet, eine präparierte PDF-Datei heruntergeladen und automatisch geöffnet, könnte eingebetteter Schadcode ausgeführt werden, was zu Datenverlusten oder anderen Problemen führen kann. Das automatische Öffnen sollte daher in den Safari-Einstellungen deaktiviert werden.

Autostart-Funktion deaktivieren
Die Funktion Autostart ermöglicht es, Programme von externen Datenträgern sofort auszuführen, wenn diese, wie zum Beispiel CDs, DVDs oder externe Festplatten, mit dem Computer verbunden werden. Da die hierdurch automatisch ausgeführten Programme auch Schadsoftware enthalten könnten, sollte diese Funktion für jeden Benutzer in den Systemeinstellungen deaktiviert werden.

Daneben gibt es weitere Konfigurationsmöglichkeiten, die aus dem Blickwinkel der Datensparsamkeit sinnvoll sind:

Liste der zuletzt verwendeten Objekte reduzieren
macOS speichert eine Liste der zuletzt verwendeten Anwendungen, Dokumente und Serververbindungen. In erster Linie erleichtern diese Informationen das Arbeiten, jedoch sind damit auch Rückschlüsse auf vertrauliche Informationen möglich, wie zum Beispiel mit welchen Dokumenten kürzlich gearbeitet wurde oder die Adressen der zuletzt benutzten Server. Um diese Informationen auf ein Minimum zu beschränken, sollte in den Systemeinstellungen die Anzahl der zuletzt verwendeten Objekte reduziert bzw. auf 0 gesetzt werden.

Sicheres Entleeren des Papierkorbes aktivieren
Um zu verhindern, dass gelöscht geglaubte Dateien aus dem Papierkorb unter macOS wiederhergestellt werden können, sollte der Papierkorb regelmäßig entleert werden. macOS bietet zudem die Einstellung "Sicheres Entleeren" an, bei der das Betriebssystem die Dateien nach dem Entleeren des Papierkorbs mit einem Bitmuster überschreibt. Um diese Einstellung zu aktivieren, muss im Finder die Einstellung "Papierkorb sicher entleeren" aktiviert werden.

SYS.2.4.M6 Verwendung aktueller Mac-Hardware (S)

Bei der Anschaffung von neuen Macs sollte auf aktuelle Modelle zurückgegriffen werden. Beim Einsatz von vorhandenen Macs sollte überprüft werden, ob diese weiterhin von Apple mit Software-Updates versorgt werden. Leider stellt Apple keine offiziellen Informationen über einen Software-Product-Lifecycle (SPL) von macOS zur Verfügung. Die Vergangenheit hat gezeigt, dass Apple mindestens zwei Jahre Sicherheitsupdates für macOS bereitstellt. Da derzeit jährlich eine neue Hauptversion von macOS erscheint, werden somit in der Regel die beiden vorhergehenden Hauptversionen zumindest mit Sicherheitsupdates versorgt. Deshalb ist es sinnvoll, andere Informationsquellen sowie Erfahrungswerte zu nutzen. Beispielsweise ist es empfehlenswert, verschiedene Webseiten und Blogs zu prüfen, die sich mit dem Thema macOS auseinandersetzen. Nach Möglichkeit sollte stets die neuste Version von macOS genutzt werden.

SYS.2.4.M7 Zwei-Faktor-Authentisierung für Apple-ID (S)

Die Zwei-Faktor-Authentisierung für die Verwendung des Apple-ID-Kontos sollte aktiviert werden. Bei diesem Authentisierungsverfahren wird bei bestimmten Aktionen neben dem Kennwort eine zusätzliche PIN abgefragt. Diese PIN erhält der Nutzer über ein registriertes vertrauenswürdige iOS-Gerät oder über eine SMS an die hinterlegte Mobilfunknummer (falls kein iOS-Gerät vorhanden ist). Die Zwei-Faktor-Authentisierung ist momentan nur für Macs geeignet, da nur hier die Authentisierung mittels zweier unabhängiger Komponenten (Mac und iOS-Gerät) stattfindet. Die Zwei-Faktor-Authentisierung für eine bestimmte Apple-ID kann auf der Webseite "appleid.apple.com" eingerichtet werden.

SYS.2.4.M8 Keine Nutzung von iCloud für schützenswerte Daten (S)

Eine Synchronisation der Daten zwischen mehreren Geräten über den iCloud-Dienst "Handoff" sollte verhindert werden, da damit sensible Daten die eigene Kontrolle verlassen. Die Geräte sollten daher immer über selbst betriebene Dienste synchronisiert werden. Sensible Daten sollten nicht in iCloud gespeichert werden. Das automatische Speichern von Entwürfen (E-Mails, Dokumente etc.) in iCloud sollte deaktiviert werden. iCloud selbst kann in den Systemeinstellungen von macOS deaktiviert werden, falls bei der Einrichtung des macOS-System iCloud aktiviert worden ist. Des Weiteren sollte sichergestellt werden, dass die Funktion "Handoff" unter "Allgemein" in den Systemeinstellungen deaktiviert ist.

SYS.2.4.M9 Verwendung von zusätzlichen Schutzprogrammen unter macOS (S)

Apple bietet mit Xprotect in macOS einen integrierten Schutz vor Schadprogrammen. Darüber hinaus existieren Virenschutz-Lösungen von Drittanbietern, die bei Bedarf eingesetzt werden sollten. Beispielsweise könnte in heterogenen Umgebungen ein zusätzliches Virenschutz-Programm eingesetzt werden, um IT-Systeme mit anderen Betriebssystemen (z. B. Windows) bei der Weitergabe von Daten zu schützen. Bei dem Einsatz eines Virenschutz-Programmes muss darauf geachtet werden, dass dessen Signaturen regelmäßig aktualisiert werden. Das Viren-Schutzprogramm sollte im Hintergrund laufen und mindestens beim Zugriff auf eine Datei eine Virenüberprüfung durchführen. Weitere Informationen sind im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* zu finden. Dabei sollte beachtet werden, dass das Viren-Schutzprogramm auch Schadsoftware für Windows-Systeme erkennt, damit gefahrlos mit Windows-Systemen kommuniziert werden kann.

SYS.2.4.M10 Aktivierung der Personal Firewall unter macOS (S)

macOS enthält eine integrierte Personal Firewall, die jedoch im Auslieferungszustand deaktiviert ist. Um den Mac vor unerwünschten Netzwerk-Zugriffen zu schützen, sollte die Personal Firewall aktiviert und konfiguriert werden.

Konfiguration der Personal Firewall
Bevor die Personal Firewall unter macOS eingesetzt wird, müssen zwei Fakten überprüft werden. Mit der Personal Firewall können ein- oder ausgehende Verbindungen gefiltert werden oder der Zugriff von Programmen und Diensten auf das Internet eingeschränkt werden. Bevor für einzelne Anwendungen die Netzkommunikation abgeschaltet wird, sollte geprüft werden, ob es möglich ist, die Netzkommunikation programmintern abzuschalten. Außerdem sollte geprüft werden, ob bei dem jeweiligen Programm oder Dienst nach dem Sperren der Netzkommunikation keine unerwünschten Nebeneffekte auftreten. Wird direkt versucht, mit einer Personal Firewall die Netzkommunikation eines Programms zu unterbinden, können Probleme auftreten, da ein Programm auf die Netzkommunikation angewiesen sein kann und auf eine Antwort aus dem Netz wartet, bevor es weiter ausgeführt wird.

Der Einsatz einer Personal Firewall, die direkt auf dem zu schützenden Client betrieben wird, ersetzt in keinem Fall ein eigenständiges Sicherheitsgateway (Firewall), dass das gesamte interne Netz der Institution schützt. Um aber beispielsweise macOS-Geräte vor Angriffen aus dem lokalen Netz zu schützen, kann der Einsatz einer Personal Firewall sinnvoll sein. Beim mobilen Einsatz von macOS-Geräten ist die Nutzung einer Personal Firewall immer empfehlenswert, um den Rechner vor Angriffen aus dem Internet zu schützen.

Vor dem Einsatz einer Personal Firewall muss festgelegt werden, welche Programme Netzzugriff erhalten sollen und welche nicht. Generell ist zunächst jegliche Netzkommunikation zu blockieren, im zweiten Schritt werden nur die gewünschten Ports oder Anwendungen freigeschaltet.

Integrierte Anwendungsfirewall
Die Anwendungsfirewall ermöglicht das Sperren und das Freigeben der Kommunikation von bestimmten Anwendungsprogrammen. Dazu muss der Anwender nicht wissen, welche Ports verwendet werden. Die Anwendungsfirewall überprüft auch die Signatur eines Programms. Es ist nicht möglich, ein für die Netzkommunikation freigegebenes Programm zu manipulieren, ohne dass eine erneute Firewall-Regeldefinition abgefragt wird. Unter macOS ist die Anwendungsfirewall im Auslieferungszustand deaktiviert. Diese muss in den Systemeinstellungen aktiviert werden. Über den Menüpunkt "Optionen" ist es möglich, die Einstellungen anzupassen.

Mit der Option "Alle eingehenden Verbindungen blocken" werden zunächst nur unbedingt notwendige macOS-Datenverbindungs- bzw. Kommunikationsdienste erlaubt, wie DHCP und Bonjour. Werden Freigaben wie beispielsweise "Dateifreigabe" oder "Entferne Anmeldung" aktiviert, öffnet macOS selbstständig die notwendigen Ports in der Firewall, über den die Dienste kommunizieren können.

Wird die Option "Alle eingehenden Verbindungen blocken" nicht verwendet, wird über die Liste der Anwendungsfirewall definiert, welche Dienste und Programme zum Öffnen von Ports in der Firewall berechtigt sind. Mit einem Mausklick auf das "+"-Symbol können Programme dieser Liste hinzugefügt werden. Nachdem ein Programm zu dieser Liste hinzugefügt wurde, muss definiert werden, ob eingehende Verbindungen für dieses Programm erlaubt oder blockiert werden sollen. Auch Befehlszeilenprogramme können zu dieser Liste hinzufügt werden. Beim Hinzufügen einer Anwendungssoftware zu dieser Liste ergänzt macOS das Programm um eine digitale Signatur, falls dies nicht zuvor schon einmal geschehen ist. Wird ein Programm nachträglich verändert, dass sich in der Liste befindet, wird der Anwender erneut aufgefordert, für das Programm eingehende Netzverbindungen zu erlauben oder zu blockieren. Auch für Programme ohne digitale Signatur, die sich nicht in dieser Liste befinden, wird dem Anwender ein Dialogfeld mit Optionen zum Erlauben oder Blockieren von Verbindungen angezeigt. Sobald der Anwender die Verbindungen erlaubt oder blockiert, versieht macOS das Programm mit einer digitalen Signatur und fügt es automatisch, einschließlich der vergebenen Berechtigungen, zur Liste der Anwendungsfirewall hinzu.

Wird die Option "Signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen" aktiviert, können alle Programme, die mit einer digitalen Signatur versehen sind, eingehende Verbindungen

empfangen, auch wenn die Programme nicht in der Liste angezeigt werden. Diese digitale Signatur muss von einer Zertifizierungsstelle (CA) ausgestellt worden sein, der Apple vertraut. Jede ausführbare Betriebssystemkomponente von macOS wurde durch Apple mit einer digitalen Signatur versehen und kann eingehende Verbindungen empfangen. Auch digital signierte Programme, die automatisch von anderen Programmen geöffnet werden, können zu dieser Gruppe gehören. Soll der Netzzugriff eines Programms mit einer digitalen Signatur über die Firewall blockiert werden, muss das Programm zuerst zur Anwendungsfirewall-Liste hinzufügt und dann ausdrücklich die Verbindungen blockiert werden. Wird der Zugriff eines Programms über die Firewall blockiert, kann das zu Störungen des Programms oder anderer, darauf basierender Programme führen oder die Leistung anderer verwendeter Programme und Dienste beeinflussen. Da diese Option nicht transparent ist, sollte von der Verwendung abgesehen werden.

Die Option "Tarn-Modus aktivieren" sollte nicht verwendet werden, da diese Option dem Internetstandard RFC 1122 widerspricht. Durch einen aktivierten Tarn-Modus werden keine Antworten auf Anfragen gesendet, die von einer blockierten Anwendung ausgehen. Ping ist beispielsweise eine der ICMP-Nachrichten, die durch den Tarnmodus nicht mehr funktionieren. Der Tarn-Modus bietet darüber hinaus aber keinen Schutz. Wäre der Rechner tatsächlich nicht vorhanden, würde die letzte Station vor dem Rechner an den Sender melden, dass das Ziel nicht erreichbar ist. Im Tarnmodus kommt jedoch keine Nachricht zurück. Daraus kann der Sender schließen, dass der Rechner da ist, aber nicht antwortet.

Deaktivieren nicht benötigter Netzdienste
Nicht benötigte Netzdienste sollten deaktiviert werden, da diese Systemressourcen belegen und ein Angriffsziel darstellen können. Dazu sind Administratorrechte notwendig. Wurden Veränderungen an den Systemdiensten vorgenommen, sind diese zu dokumentieren. Weiterhin sollte regelmäßig überprüft werden, ob nur nach dem Sicherheitskonzept zulässige Dienste aktiviert und über das Netz erreichbar sind.

Die verfügbaren Dienste werden in den Systemeinstellungen unter dem Menüpunkt "Freigaben" aufgelistet. Im Regelfall sollte ein Client-Betriebssystem keine oder nur wenige Dienste in einem Netz anbieten. Je nach Einsatzgebiet muss eine individuelle Entscheidung getroffen werden, ob und welcher Dienst aktiviert bleiben sollte.

Zur Verwaltung verwendete Dienste, wie zum Beispiel der "Apple Remote Desktop" (TCP-Port 5900), "Entfernte Anmeldung" (SSH-Zugriff, TCP-Port 22) oder Netzdienste des Viren-Schutzprogramms müssen aktiviert bleiben.

Wird in einem Netz der Dienst "Bonjour" nicht verwendet, sollte dieser ebenfalls deaktiviert werden, da er Systemressourcen belegt und einen weiteren Angriffspunkt darstellt.

sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist

sudo launchctl unload -w/System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.plist

Wird das Betriebssystem aktualisiert, könnten Dienste unbeabsichtigt wieder aktiviert werden. Daher sollte nach jeder Aktualisierung geprüft werden, ob die Dienste weiterhin deaktiviert sind.

SYS.2.4.M11 Geräteaussonderung von Macs (S)

Daten müssen von nicht mehr verwendeten Geräten gelöscht werden. Unverschlüsselte und verschlüsselte Festplatten müssen vor einer Geräteaussonderung vollständig überschrieben werden. Darüber hinaus sollte der nichtflüchtige Datenspeicher des Macs (NVRAM, Non-Volatile Random-Access Memory) zurückgesetzt werden. Der NVRAM dient dazu, verschiedene Einstellungen (z.B. Daten für die WLAN-Authentisierung) des Macs zu speichern.

Aussonderung eines macOS Systems
Auf ausgesonderten Arbeitsplatz-PCs müssen alle sensiblen Informationen auf geeignete Weise gelöscht werden. Dies gilt auch für Informationen auf defekten Datenträgern. Wurden auf einem Datenträger sensible Informationen abgelegt und kann durch einen Hardware-Fehler nicht mehr auf den Datenträger zugegriffen werden, so muss der Datenträger in geeigneter Weise zerstört werden.

Um unter macOS Informationen zu löschen, kann das "Festplatten-Dienstprogramm" verwendet werden. Handelt es sich um den Datenträger mit der Systempartition, muss der Computer von einem macOS-

Installationsmedium oder über die Recovery-Funktion gestartet und das "Festplatten-Dienstprogramm" aufgerufen werden. Mit diesem Programm lässt sich ein Datenträger auf unterschiedliche Arten löschen. In den Sicherheitsoptionen sollte "Daten mit Nullen überschreiben" eingestellt werden. Die Administratoren müssen im Umgang mit dem "Festplatten-Dienstprogramm" geschult und über die Vorgehensweise des sicheren Löschens von Datenträgern unter macOS informiert werden.

Bevor IT-Systeme oder Datenträger ausgesondert werden, müssen sie gesichtet werden, ob sich darauf noch benötigte Daten befinden. Diese müssen dann auf anderen Datenträgern gesichert bzw. archiviert werden. Es sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden.

SYS.2.4.M12 Firmware-Kennwort und Boot-Schutz auf Macs (H)

Um ein unberechtigtes Booten des Macs zu verhindern, sollte das Firmware-Kennwort aktiviert werden. Sofern dieses aktiviert ist, können ohne Authentisierung außerdem keine Änderungen an den Einstellungen, wie den Bootoptionen, durchgeführt werden.

Das Firmware-Passwort kann in zwei verschiedenen Modi gesetzt werden:

Command-Modus: Die Firmware fragt beim Bootvorgang nach einem Passwort, wenn der Benutzer versucht, von einem anderen Startlaufwerk zu booten. Wenn der Rechner ganz normal gestartet wird, erfolgt keine Passwortabfrage.

Full-Modus: Wenn dieser Modus gesetzt ist, wird bei jedem Start des Rechners nach dem Passwort gefragt, also auch beim ganz normalen OS-Bootvorgang.

Firmware-Passwörter können unter macOS nur über "/usr/sbin/firmwarepasswd" gesetzt werden. Dafür sind Administrationsrechte Voraussetzung. Auf der Recovery-Partition gibt es eine GUI-Applikation namens "Firmware-Passwortdienstprogramm", die ebenfalls das Firmware-Passwort setzt, jedoch nur im Command-Modus.

Nicht zu verwechseln ist das Firmware-Passwort mit der vierstelligen “iCloud-PIN“, die nach dem Sperren eines Macs durch die Funktion "Find My Mac" angezeigt wird. Der grundsätzliche Wirkmechanismus ist jedoch gleich, der Mac setzt seine Arbeit erst fort, wenn die korrekte PIN eingegeben wurde.

Auf Macs mit T2-Sicherheitschip sollte ein Firmware-Passwort über das Startsicherheitsdienstprogramm gesetzt werden. Die Optionen „Sicheres Starten: Volle Sicherheit“ sowie „Starten von externen Medien nicht zulassen“ sollten aktiviert werden.

3. Weiterführende Informationen

3.1 Wissenswertes

Ergänzende Informationen liefert das folgende Dokument:

NIST Special Publication 800-179: Guide to Securing Apple OS X 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist

3.2 Quellenverweise

Für diese Umsetzungshinweise sind keine Quellenverweise vorhanden.