jamf

WHITE PAPER

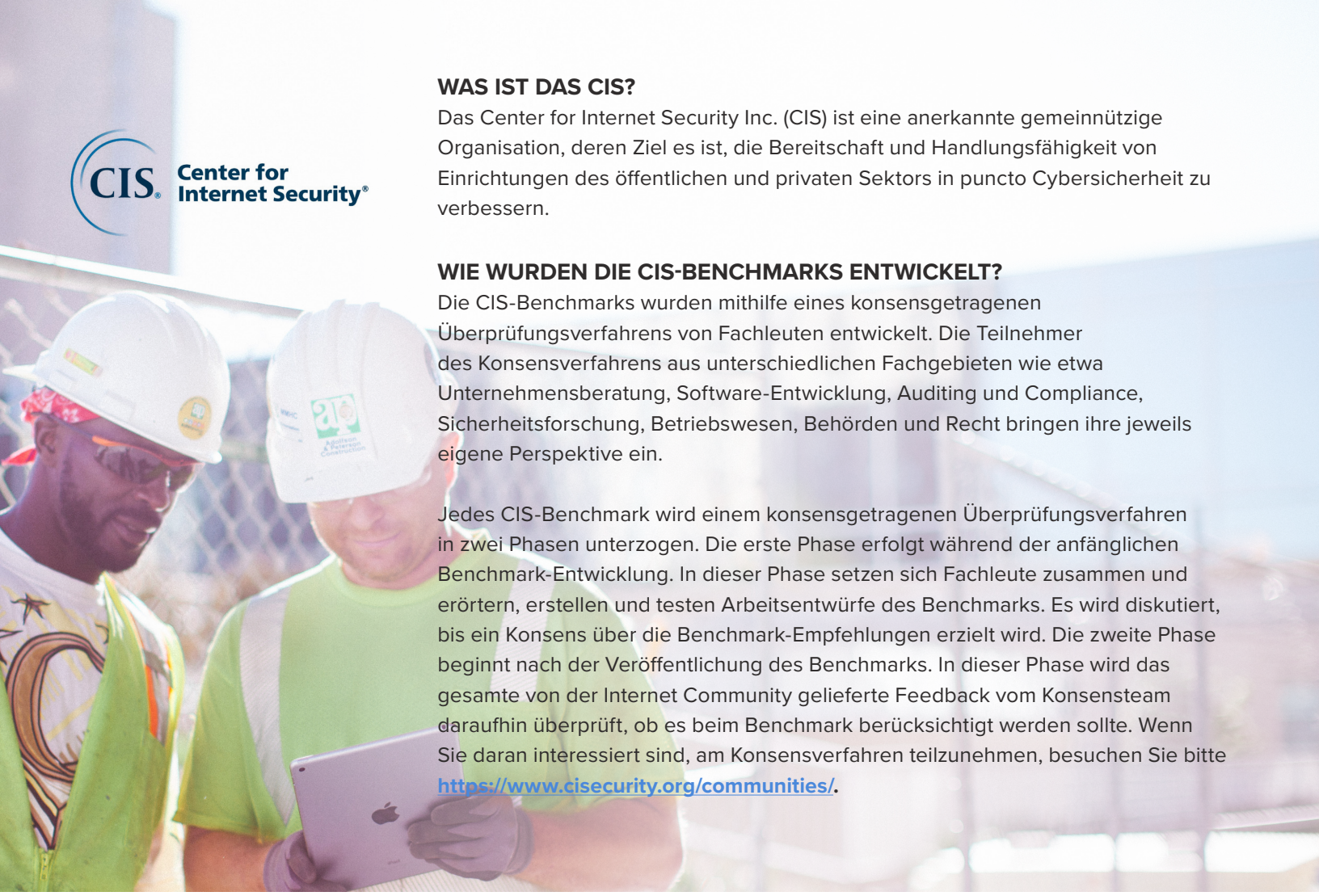
Sicherheitscheckliste für iOS

Implementierung der vom Center for Internet Security herausgegebenen Benchmarks für iOS

Empfehlungen für die Absicherung von iOS

Die vom Center for Internet Security herausgegebenen Benchmarks für iOS gelten allgemein als umfassende Checkliste für Organisationen, um iPad und iPhone abzusichern. Dieses Whitepaper erläutert, wie man die Empfehlungen der unabhängigen Organisation umsetzt.

Informationen darüber, wie Jamf Pro dazu beitragen kann, Ihre iOS Geräte abzusichern und zu verwalten, finden Sie unter **jamf.com/de**



WAS IST DAS CIS?

Das Center for Internet Security Inc. (CIS) ist eine anerkannte gemeinnützige Organisation, deren Ziel es ist, die Bereitschaft und Handlungsfähigkeit von Einrichtungen des öffentlichen und privaten Sektors in puncto Cybersicherheit zu verbessern.

WIE WURDEN DIE CIS-BENCHMARKS ENTWICKELT?

Die CIS-Benchmarks wurden mithilfe eines konsensgetragenen Überprüfungsverfahrens von Fachleuten entwickelt. Die Teilnehmer des Konsensverfahrens aus unterschiedlichen Fachgebieten wie etwa Unternehmensberatung, Software-Entwicklung, Auditing und Compliance, Sicherheitsforschung, Betriebswesen, Behörden und Recht bringen ihre jeweils eigene Perspektive ein.

Jedes CIS-Benchmark wird einem konsensgetragenen Überprüfungsverfahren in zwei Phasen unterzogen. Die erste Phase erfolgt während der anfänglichen Benchmark-Entwicklung. In dieser Phase setzen sich Fachleute zusammen und erörtern, erstellen und testen Arbeitsentwürfe des Benchmarks. Es wird diskutiert, bis ein Konsens über die Benchmark-Empfehlungen erzielt wird. Die zweite Phase beginnt nach der Veröffentlichung des Benchmarks. In dieser Phase wird das gesamte von der Internet Community gelieferte Feedback vom Konsensteam daraufhin überprüft, ob es beim Benchmark berücksichtigt werden sollte. Wenn Sie daran interessiert sind, am Konsensverfahren teilzunehmen, besuchen Sie bitte **https://www.cisecurity.org/communities/**.

CIS und iOS Management

WAS IST MDM?

Mobile Device Management (MDM) ist die integrierte Verwaltungsarchitektur von Apple für iOS, macOS und tvOS. Jamf Pro ist die Standardlösung für Apple MDM.

GERÄTEEIGENTÜMERSCHAFT

Die Sicherheitsanforderungen sind je nach Technologiemodell des Unternehmens unterschiedlich: Geräte im Privatbesitz, die im Rahmen einer BYOD-Initiative (Bring Your Own Device) genutzt werden, oder Geräte im Unternehmensbesitz, die an die Benutzer verteilt werden.

WAS SIND KONFIGURATIONSPROFILE?

Mithilfe von Konfigurationsprofilen werden Einstellungen auf iOS Geräten definiert. Sie werden per MDM an die Geräte verteilt.

SICHERHEITSSTUFE

Level 1 (L1) bzw. Level 2 (L2) definieren die Sicherheitsanforderungen und -einstellungen, die für ein Gerät im Privatbesitz bzw. im Unternehmensbesitz angewendet werden müssen. Bei L2 unterliegt das Gerät einer stärkeren Kontrolle, die über grundlegende Sicherheitsanforderungen hinausgeht.

WAS VERSTEHT MAN UNTER BETREUUNG?

Die Betreuung umfasst eine intensivere Verwaltung von iOS Geräten, die über Apple Bereitstellungsprogramme oder Apple Configurator zur Verwaltung registriert wurdenr.

WAS IST APNs?

Der Apple Push Notification Service (APNs) ist für die iOS Verwaltung erforderlich. Bitte lesen Sie den folgenden Artikel, um weitere Informationen über APNs zu erhalten https://www.jamf.com/blog/what-is-apple-push-notification-service-apns/ requirements.

Absicherung von Geräten im Unternehmensbesitz

Laut einer vor Kurzem durchgeführten Umfrage würden 74 % der Mitarbeiter von Unternehmen für die Arbeit ein vom Unternehmen bereitgestelltes Gerät einem eigenen Gerät vorziehen.* Jamf Pro unterstützt Organisationen dabei, ihr Programm für iOS Geräte im Unternehmensbesitz auf sichere Weise umzusetzen. Sie werden dadurch in die Lage versetzt, die Verteilung und Verwaltung von iPad und iPhone Geräten im Unternehmensbesitz zu optimieren.

Empfehlungen des CIS

Einrichtung:

- Einwilligungsmeldung und Beschreibung des Registrierungsprofils festlegen
- Sicherstellen, dass das Profil entfernt werden kann.

Funktionalität:

- **L2:** Bildschirmfotos und Bildschirmaufzeichnung deaktivieren
- Sprachwahl deaktivieren, wenn Gerät gesperrt ist
- Siri deaktivieren, wenn Gerät gesperrt ist
- iCloud-Backup deaktivieren
- iCloud-Dokumente und -Daten deaktivieren
- iCloud-Schlüsselbund deaktivieren
- Bei verwalteten Apps das Sichern von Daten in iCloud deaktivieren
- Verschlüsselte Backups erzwingen
- „Alle Inhalte und Einstellungen erlauben“ deaktivieren
- L2: Benutzer dürfen keine nicht vertrauenswürdigen TLS-Zertifikate annehmen
- Installation von Konfigurationsprofilen nicht erlauben
- Hinzufügen von VPN-Konfigurationen nicht erlauben
- Änderung der App-Einstellungen für mobile Daten nicht erlauben
- L2: Verbindung mit Hosts ohne Configurator-Installation nicht erlauben
- Dokumente aus verwalteten Quellen in unverwalteten Zielen nicht erlauben
- Dokumente aus unverwalteten Quellen in verwalteten Zielen nicht erlauben
- Das Behandeln von AirDrop als unverwaltetes Ziel aktivieren
- Handoff nicht erlauben
- Apple Watch Handgelenkerkennung durchsetzen
- Einrichtung neuer Geräte in der Nähe nicht erlauben
- Anzeige des Kontrollzentrums im Sperrbildschirm deaktivieren
- Anzeige der Mitteilungszentrale im Sperrbildschirm deaktivieren.

Apps:

- Betrugswarnung erzwingen
- „Cookies akzeptieren“ ist auf „Von Websites, die ich besuche“ oder „Nur von aktueller Website“ eingestellt

Domains:
- Verwaltete Safari Web Domains konfigurieren.

Passwörter:
- Einfache Werte nicht erlauben.
- Mindestlänge des Codes ist auf „6“ eingestellt.
- „Automatische Sperre (max.)“ ist auf maximal „2 Minuten“ eingestellt.
- „Maximale Zeitgrenze für Gerätesperrung“ ist auf „Sofort“ eingestellt.
- „Maximale Anzahl von Fehlversuchen“ ist auf „6“ eingestellt.

VPN:
- Sicherstellen, dass VPN „konfiguriert“ ist.
- Vorzugsweise ist App-basiertes VPN zu verwenden.

Mail:
- E-Mail-Account des Benutzers mit einem E-Mail-Profil einrichten.
- Benutzern nicht erlauben, Nachrichten von diesem Account zu verschieben.

Mitteilungen:
- Mitteilungseinstellungen für alle verwalteten Apps konfigurieren.

Lock Screen Message:
- Nachricht „Bei Verlust bitte senden an“ konfigurieren.

Funktionen von Jamf Pro

Mit Jamf Pro können Sie alle oben genannten L1- und L2-Systemeinstellungen mithilfe von Konfigurationsprofilen einrichten, aktivieren bzw. deaktivieren. Für einige dieser Einstellungen muss das iOS Gerät bei der Registrierung betreut werden.
Im Folgenden finden Sie weitere Informationen zur iOS Betreuung: https://support.apple.com/en-us/HT202837.

Jamf Pro ermöglicht es Organisationen darüber hinaus, eine individuelle Sperrbildschirm-Nachricht einzurichten, damit die Geräte auf sichere Weise zurückgegeben und nicht entsperrt und manipuliert werden.

*Source: https://www.jamf.com/resources/e-books/survey-the-impact-of-device-choice-on-the-employee-experience/

Absicherung von BYOD-Geräten und Geräten im Privatbesitz

Empfehlungen des CIS

Einrichtung:

- Einwilligungsmeldung und Beschreibung des Registrierungsprofils festlegen
- Sicherstellen, dass das Profil entfernt werden kann.

Funktionalität:

- Sprachwahl deaktivieren, wenn Gerät gesperrt ist
- Siri deaktivieren, wenn Gerät gesperrt ist
- Bei verwalteten Apps das Sichern von Daten in iCloud deaktivieren
- Verschlüsselte Backups erzwingen
- L2: Benutzer dürfen keine nicht vertrauenswürdigen TLS-Zertifikate annehmen
- Dokumente aus verwalteten Quellen in unverwalteten Zielen nicht erlauben
- Dokumente aus unverwalteten Quellen in verwalteten Zielen nicht erlauben
- Das Behandeln von AirDrop als unverwaltetes Ziel aktivieren
- L2: Handoff nicht erlauben
- Anzeige des Kontrollzentrums im Sperrbildschirm deaktivieren
- Anzeige der Mitteilungszentrale im Sperrbildschirm deaktivieren.

Apps:

- Betrugswarnung in Safari erzwingen.
- „Cookies akzeptieren“ ist auf „Von Websites, die ich besuche“ oder „Nur von aktueller Website“ eingestellt.

Domains:

- Verwaltete Safari Web Domains konfigurieren.

Passwörter:

Einfache Werte nicht erlauben

- Mindestlänge des Codes ist auf „6“ eingestellt.
- „Automatische Sperre (max.)“ ist auf maximal „2 Minuten“ eingestellt
- „Maximale Zeitgrenze für Gerätesperrung“ ist auf „Sofort“ eingestellt
- „Maximale Anzahl von Fehlversuchen“ ist auf „6“ eingestellt.

VPN:

- Sicherstellen, dass VPN „konfiguriert“ ist
- Vorzugsweise ist App-basiertes VPN zu verwenden.

Mail:

- E-Mail-Account des Benutzers mit einem E-Mail-Profil einrichten
- Benutzern nicht erlauben, Nachrichten von diesem Account zu verschieben.

Mitteilungen:

- Sicherstellen, dass VPN „konfiguriert“ ist
- Vorzugsweise ist App-basiertes VPN zu verwenden.

Funktionen von Jamf Pro

Mit der BYOD-Lösung von Jamf Pro können Sie eine eigene Einwilligungsmeldung und Beschreibung des Registrierungsprofils festlegen. Die Lösung bietet ein einfaches Verfahren, mit dem ehemalige Mitarbeiter das BYOD-Profil entfernen können, wenn sie aus dem Unternehmen bzw. dem Programm ausscheiden.

Falls Sie in Ihrem Unternehmen alle von der CIS empfohlenen L1- bzw. L2-Sicherheitseinstellungen implementieren müssen, nutzen Sie bitte die Funktion von Jamf Pro, das iOS Gerät als nicht betreutes Gerät im Unternehmensbesitz zu registrieren. Wir empfehlen zudem, die Einstellung für die benutzerinitiierte Registrierung von iOS Geräten im Privatbesitz zu deaktivieren. Durch das Erstellen von Konfigurationsprofilen mit Jamf Pro können sämtliche L1- und L2-Sicherheitseinstellungen für einzelne iOS Geräte oder für Gruppen von iOS Geräten konfiguriert, deaktiviert bzw. aktiviert werden.

Weitere Überlegungen

Jamf Pro unterstützt Unternehmen dabei, über das Gerätemanagement und die Konfigurationsprofile hinauszugehen, indem sichergestellt wird, dass die Geräte immer mit der neuesten Software ausgestattet sind und die Tore nicht für böswillige Angriffe offen stehen.

Empfehlungen des CIS:

- Sicherstellen, dass beim iOS Gerät kein Jailbreak durchgeführt wurde
- Software auf dem neuesten Stand halten
- Automatische Downloads von App-Updates aktivieren
- „Mein iPad suchen“ bzw. „Mein iPhone suchen“ ausschließlich auf Geräten von Endanwendern aktivieren
- Sicherstellen, dass bei Personen, auf deren Geräte wichtige Informationen gespeichert sind, die aktuellste iOS Gerätearchitektur verwendet wird.

Funktionen von Jamf Pro

Jamf Pro bietet für das Betriebssystem von iPad und iPhone Support ab der allerersten Version. So wird sichergestellt, dass immer die aktuellste Software unterstützt wird. Zudem können Organisationen mithilfe von Jamf Pro Self Service einen eigenen Katalog mit individuell angepassten Apps und allen Ressourcen, Apps und Konfigurationen erstellen, die die Benutzer möglicherweise benötigen. Den Benutzern wird On-Demand-Zugriff gewährt, und zwar ohne dass sie bei der IT-Abteilung eine Supportanfrage einreichen müssen. Bei Verlust oder Diebstahl kann das Gerät mit Jamf Pro auf sichere Weise gesperrt, gelöscht und zurückgesetzt werden. So ist sichergestellt, dass Unternehmensdaten und private Daten nie in falsche Hände gelangen können.

Bessere Gerätesicherheit beginnt hier

Mit Jamf Pro ist es ganz einfach, die Apple iOS Benchmarks der unabhängigen Organisation „Center for Internet Security“ umzusetzen und zu befolgen.

Setzen Sie diesen Leitfaden in die Praxis um, indem Sie eine kostenlose Testversion anfordern.

jamf

Um mehr darüber zu erfahren, wie sie Jamf Pro für die Verwaltung Ihrer Macs oder iOS nutzen können, besuchen Sie **jamf.com/de**

www.jamf.com