jamf

WHITEPAPER

Sicherheitscheckliste für macOS:

Implementierung des Center for Internet Security Benchmark für macOS

Empfehlungen für die Sicherung von macOS

Der Center for Internet Security (CIS) Benchmark für macOS gilt weithin als umfassende Checkliste für Unternehmen zur Absicherung ihrer Macs. Dieses Whitepaper von Jamf - the Standard for Apple Enterprise Management - zeigt Ihnen, wie Sie die Empfehlungen der unabhängigen Organisation umsetzen können.

jamf PRO

WAS IST JAMF PRO?

Jamf Pro ist ein Paket von Verwaltungstools, das Ihnen bei der Verwaltung Ihrer Apple Geräte hilft.

jamf PROTECT

WAS IST JAMF PROTECT?

Jamf Protect ist eine Endpoint-Sicherheitslösung, die speziell für Apple und die Macs von Unternehmen entwickelt wurde.

jamf CONNECT

WAS IST JAMF CONNECT?

Jamf Connect bietet eine einzige Cloud Identität auf jedem Apple Gerät, um sofortigen Zugriff auf die benötigten Ressourcen zu erhalten.

CIS Center for Internet Security®

WER IST DAS CENTER FOR INTERNET SECURITY?

Das Center for Internet Security, Inc. (CIS) ist eine gemeinnützige Organisation (501(c)(3)), deren Ziel es ist, die Bereitschaft und Reaktionsfähigkeit öffentlicher und privater Einrichtungen im Bereich der Internetsicherheit zu verbessern.

WIE DER CIS-BENCHMARK ERSTELLT WURDE

Die CIS-Benchmark wurde im Rahmen eines Konsensprüfungsverfahrens erstellt , an dem Fachleute beteiligt waren. Die Konsens-Teilnehmer*innen kommen aus unterschiedlichen Bereichen wie Beratung, Softwareentwicklung, Audit und Compliance, Sicherheitsforschung, Betrieb, Regierung und Recht.

Jede 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 werden alle Rückmeldungen aus der Gemeinschaft vom Konsensfindungsteam geprüft und in den Benchmark eingearbeitet. Wenn Sie an einer Teilnahme am Konsensverfahren interessiert sind, besuchen Sie bitte **https://community.cisecurity.org**.

JAMF PROTECT UND CIS

Jamf Protect hat kürzlich die CIS Benchmark-Zertifizierung von CIS erhalten. Unternehmen, die Jamf Protect nutzen, können nun sicherstellen, dass die Konfigurationen ihrer kritischen Anlagen mit den konsensbasierten CIS Benchmark-Praxisstandards für macOS übereinstimmen.

CIS gibt Empfehlungen für verschiedene macOS Kategorien, in denen Einstellungs-kontrollen implementiert werden sollten, um die Möglichkeit der Datenexfiltration zu verringern.

Während Jamf Pro Ihnen die Möglichkeit und die Werkzeuge gibt, die CIS-Empfehlungen zu befolgen, automatisiert Jamf Protect die Bewertung der wesentlichen CIS-Sicherheitseinstellungen auf einer täglichen Basis, um die Konformität und Audit-Überwachung über den Benchmark für macOS und die Sicherheitsprioritäten Ihres Unternehmens zu validieren.

Kategorien der macOS Sicherheit

AKTUALISIERUNGEN & PATCHES

SYSTEMPRÄFERENZEN

ICLOUD

PROTOKOLLIERUNG & PRÜFUNG

NETZWERK-KONFIGURATIONEN

BENUTZERKONTEN

ZUGANG & AUTHENTIFIZIERUNG

ANDERE ÜBERLEGUNGEN

Installation von Aktualisierungen, Patches und Sicherheitssoftware

Mit Jamf Pro können Sie Ihr macOS und Ihre Programme auf dem neuesten Stand halten, indem Sie Aktualisierungen paketieren und per Fernzugriff auf Ihre Client Macs verteilen. Sie können sogar einen Bericht erstellen, um den Status von macOS Upgrades in Echtzeit zu überwachen und sicherzustellen, dass Ihre Mac Flotte mit dem neuesten und sichersten Betriebssystem arbeitet.

CIS-Benchmark-Empfehlungen:

- Überprüfen Sie, ob die von Apple bereitgestellte Software aktuell ist
- Automatische Aktualisierungen einschalten
- Installationen von App-Updates aktivieren
- Aktivieren von Systemdatendateien und Sicherheitsaktualisierungs-Installationen
- Aktivieren Sie die Installation von macOS Aktualisierungen

Funktionen von Jamf Pro:

- Das Patch-Management hilft Ihnen dabei, Ihr macOS und Ihre beliebten Apps mit den neuesten Versionen auf dem neuesten Stand zu halten.
- Mit einem benutzerdefinierten Software Update Server können Sie zugelassene Aktualisierungen für Ihre Macs auf eine Whitelist setzen
- Führen Sie eine Richtlinie aus, um die automatische Aktualisierung über den App Store zu aktivieren
- Führen Sie eine Richtlinie aus, um auf einem Client Mac nach Aktualisierungen zu suchen

Funktionen in Jamf Connect:

- Erfordert einen Cloud Benutzernamen und ein Passwort
- Gastkonten werden ausgeblendet
- Keine Passwort-Hinweise für lokale Konten

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen, um die Compliance mit Aktualisierungen, Patches und Sicherheits-Software zu überprüfen

Systempräferenzen

Jamf Pro hilft Ihnen, die Systemeinstellungen so zu konfigurieren, dass sie den Sicherheitsanforderungen Ihres Unternehmens gerecht werden: Allgemeine und erweiterte Einstellungen können für Ihre gesamte Mac Flotte festgelegt werden, um Ihre Sicherheit sowohl gegen physische als auch gegen Angriffe aus der Ferne zu erhöhen.

CIS-Benchmark-Empfehlungen:

Bluetooth:
- Deaktivieren von Bluetooth
- Bluetooth-Erkennungsmodus deaktivieren

Datum & Uhrzeit:
- Automatische Einstellung von Uhrzeit und Datum aktivieren
- Sicherstellen, dass die eingestellte Zeit innerhalb angemessener Grenzen liegt

Desktop & Bildschirmschoner:
- Legen Sie ein Inaktivitätsintervall von 20 Minuten oder weniger für den Bildschirmschonerfest
- Sichere Bildschirmschoner-Ecken
- Benutzer*innen mit den Tools zur Bildschirmsperre oder der Ecke zum Start des Bildschirmschonersvertraut machen

Teilen:
- Deaktivieren von Remote Apple Events in der Freigabe
- Internetfreigabe deaktivieren
- Bildschirmfreigabe deaktivieren
- Druckerfreigabe deaktivieren
- Fernanmeldung (SSH) deaktivieren
- DVD- oder CD-Freigabe deaktivieren
- Bluetooth-Freigabe deaktivieren
- Dateifreigabe deaktivieren
- Fernverwaltung deaktivieren (ARD)

Energiesparen:
- Aufwachen für Netzwerkzugriff deaktivieren

Sicherheit & Datenschutz:
- FileVault aktivieren
- Sicherstellen, dass alle APFS-Volumes des Benutzerspeichers verschlüsseltsind
- Sicherstellen, dass alle CoreStorage-Volumes des Benutzerspeichers verschlüsselt sind
- Gatekeeper aktivieren
- Firewall aktivieren
- Firewall-Stealth-Modus aktivieren
- Überprüfung der Anwendungsfirewall-Regeln
- Aktivieren der Standortdienste
- Überwachung des Zugriffs auf Standortdienste
- Senden von Diagnose- und Nutzungsdaten an Apple deaktivieren

Andere:
- iCloud (siehe Abschnitt unten)
- Time Machine Auto-Backup
- Time Machine Volumes sind verschlüsselt
- Pairing des Infrarot-Empfängers der Fernbedienung, falls aktiviert
- Sichere Tastatureingabe in terminal.app aktivieren
- Java 6 ist nicht die Standard-Java-Laufzeitumgebung
- Sicheres Löschen von Dateien nach Bedarf
- Sicherstellen, dass die EFI-Version gültig ist und regelmäßig überprüftwird

Funktionen von Jamf Pro:

- Alle oben genannten Systempräferenzen können über eine Jamf Pro Server-Richtlinie und/oder ein -Konfigurationsprofil eingestelltwerden
- FileVault 2 kann aktiviert und der Schlüssel im Inventar Ihres Jamf Pro Servers hinterlegt werden
- Bildschirmschoner und Kennworteinstellungen können festgelegt werden
- Freigabeeinstellungen können festgelegt werden
- Sicherheits- & Datenschutzeinstellungen können festgelegt werden
- Richtlinie zur Deaktivierung von Java kann eingesetzt werden

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen , um die Übereinstimmung mit den Systemeinstellungen zu überprüfen

iCloud und andere Cloud Dienste

Jamf Pro hilft bei der Umsetzung der iCloud Strategie Ihres Unternehmens, indem es IT-Administrator*innen die Möglichkeit gibt, den Cloud basierten Dienst entweder zu blockieren oder zu aktivieren.

CIS-Benchmark-Empfehlungen

„iCloud von Apple ist ein verbraucherorientierter Dienst, der es dem Benutzer/der Benutzerin ermöglicht, Daten zu speichern sowie Geräte zu finden, zu steuern und zu sichern, die mit seiner Apple ID (Apple Konto) verbunden sind. Die Verwendung von iCloud auf Unternehmensgeräten sollte mit der Richtlinie zur akzeptablen Nutzung von Geräten, die verwaltet werden, sowie mit den Vertraulichkeitsanforderungen für Daten, die vom Benutzer/von der Benutzerin bearbeitet werden, übereinstimmen. Wenn iCloud erlaubt ist, werden die Daten, die auf Apple Server kopiert werden, wahrscheinlich sowohl auf privaten als auch auf Unternehmensgeräten dupliziert."

iCloud:

- iCloud Konfiguration
- iCloud Keychain
- iCloud Drive
- iCloud Drive Dokumentensynchronisierung
- iCloud Drive Desktop-Synchronisierung

Funktionen von Jamf Pro:

- iCloud kann mithilfe eines Konfigurationsprofilsdeaktiviert werden
- Wenn iCloud nicht erlaubt ist, kann iCloud Drive aus dem Finder entfernt werden

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen, um die Konformität für iCloud und andere Cloud Dienste zu überprüfen

Protokollierung und Prüfung

Jamf Pro kann IT-Administrator*innen dabei helfen, den Überblick über die von macOS erzeugten Protokolle zu behalten, und zentralisiert sie an einem Ort. Administrator*innen können auch erweiterte Berichte über diese Protokolle ausführen, um nach möglichen Sicherheitsproblemen zu suchen.

Empfehlungen des CIS:

- Sicherheitsprüfung aktivieren
- Sicherheitsüberwachungskennzeichen konfigurieren
- Aufrechterhaltung der Sicherheitsprüfung gewährleisten
- Kontrolle des Zugriffs auf Prüfungsunterlagen
- Install.log für 365 oder mehr Tage aufbewahren
- Sicherstellen, dass die Firewall für die Protokollierung konfiguriert ist

Funktionen von Jamf Pro:

- Konfigurationsprofile können über ein Skriptgeändert werden
- Protokolldateien können an den Jamf Pro Server gesendet und so lange wie nötig gespeichert werden
- Zusätzliche Protokolle können vom Jamf Pro Serverzwischengespeichert werden

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen, um die Konformität für Protokollierung und Auditing zu überprüfen

Netzwerk-Konfigurationen

Jamf Pro erleichtert IT-Administrator*innen die Einführung von Netzwerk-Konfigurationen durch die Verteilung von Wi-Fi-, VPN-, und sogar DNS-Einstellungen. Jamf Pro stellt auch sicher, dass einige der älteren Serverkomponenten von macOS deaktiviert sind, damit die Benutzer*innen nicht versehentlich Ports öffnen, von denen sie nichts wissen.

Empfehlungen des CIS:

- Bonjour-Werbedienst deaktivieren
- Aktivieren Sie „Wi-Fi-Status in der Menüleiste anzeigen".
- Netzwerkspezifische Standorte erstellen
- Sicherstellen, dass der http-Server nicht läuft
- Sicherstellen, dass der nfs-Server nicht läuft

Funktionen von Jamf Pro:

- Netzwerkeinstellungen können in ein Konfigurationsprofilintegriert werden
- Apache, FTP und NFS können alle über die Jamf Pro Server Richtliniendeaktiviert werden

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen , um die Compliance von Netzwerkkonfigurationen zu überprüfen

Benutzerkonten und Umgebung

Jamf Pro unterstützt Unternehmen bei der Verwaltung lokaler Accounts auf einem Mac und ermöglicht die Erstellung von Admin- oderStandardbenutzer*innen. Die Jamf Binärdatei, die sich auf den Client Computern befindet, erstellt einen versteckten Management-Account, der über Administratorrechte verfügt, um Befehle auszuführen und neue Benutzer*innen zu erstellen. Es können Richtlinien erstellt werden, um den Anmeldebildschirm weiter zu sichern und das Gastkonto zu deaktivieren.

CIS-Benchmark-Empfehlungen:

- Anmeldefenster mit Name und Passwort anzeigen
- Deaktivieren Sie „Passwort-Hinweise anzeigen"
- Anmeldung von Gastkonten deaktivieren
- Deaktivieren Sie „Gästen den Zugriff auf freigegebene Ordnergestatten".
- Gastordner entfernen
- Dateinamenerweiterungen einschalten
- Deaktivieren Sie das automatische Ausführen von sicheren Dateien in Safari
- Safari-Internet-Plugins für die globale Verwendung deaktivieren
- Verwendung von Kindersicherungen für Systeme, die nicht zentral verwaltetwerden

Funktionen von Jamf Pro:

- Das Anmeldefenster kann über das Konfigurationsprofilkonfiguriert werden
- Gastkonto kann über Jamf Pro Server Richtliniendeaktiviert werden
- Benutzerkonten können über den Einrichtungsassistenten und die Anmeldung im Apple Business Managererstellt werden
- Erstellte Konten können je nach Bedarf entweder Standard oder Admin sein

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen, um die Compliance für Benutzerkonten und Umgebung zu überprüfen

Systemzugang, Authentifizierung und Autorisierung

Jamf Pro hilft bei der Festlegung von Dateiberechtigungen, strengen Passwortrichtlinien und der Verwaltung des Keychain-Zugriffs für Benutzer*innen. Durch die Erstellung eines Konfigurationsprofils oder einer Jamf Pro Server Richtlinie können Sie die Zugriffseinstellungen des Systems aus der Ferne aktivieren, um einen sichereren Mac zu schaffen.

CIS-Empfehlungen:

Dateisystemberechtigungen und Zugriffskontrollen:

- Gesicherte Home-Ordner
- Prüfen Sie systemweite Anwendungen auf entsprechende Berechtigungen
- Systemordner auf beschreibbare Dateien prüfen
- Library-Ordner auf weltweit beschreibbare Dateien prüfen

Passwort-Verwaltung:

- Konfiguration des Schwellenwerts für die Kontosperre

- Legen Sie eine Mindestlänge für das Passwort fest
- Komplexe Passwörter müssen ein alphabetisches Zeichenenthalten
- Komplexe Passwörter müssen ein numerisches Zeichen enthalten
- Komplexe Passwörter müssen ein Sonderzeichen enthalten
- Komplexe Passwörter müssen Groß- und Kleinbuchstabenenthalten
- Passwort Alter
- Passwortverlauf
- Verkürzung der sudo-Timeout-Zeit
- Für jede Benutzer*innen/Tty-Kombinationeinen eigenen Zeitstempel verwenden
- Automatisches Sperren des Login-Keychain bei Inaktivität
- Sicherstellen, dass der Login-Keychain im Ruhezustanddes Computers gesperrt ist
- Aktivieren der OCSP- und CRL-Zertifikatsprüfung
- Das „root”-Konto nicht aktivieren
- Automatische Anmeldung deaktivieren
- Ein Passwort verlangen, um den Computer aus dem Ruhezustand oder Bildschirmschoner aufzuwecken
- Sicherstellen, dass das System in den Ruhezustand versetzt wurde
- Für den Zugriff auf systemweite Einstellungen ist ein Administrator*innen-Passwort erforderlich
- Deaktivieren der Möglichkeit, sich bei der aktiven und gesperrten Sitzungeines anderen Benutzers/einer anderen Benutzerin anzumelden
- Ein Banner für das Anmeldefenster erstellen
- Geben Sie keinen passwortbezogenen Hinweis ein
- Schnellen Benutzerwechsel deaktivieren
- Sichern Sie einzelne Keychains und Gegenstände
- Erstellen von speziellen Keychains für verschiedene Zwecke
- Status der System Integrity Protection (SIP)

Funktionen von Jamf Pro:

- Der Befehl „Berechtigungen reparieren” kann über Self Service ausgelöst oder automatisch ausgeführt werden.
- Es können Berichte erstellt werden, um Dateien in System und Bibliothek auf schlechte Berechtigungen zu prüfen
- Passwortrichtlinien über Konfigurationsprofil aktiviert
- Anmeldefenster und Banner können über die Jamf Pro Server Policy hinzugefügt werden
- Ordnerberechtigungen können über ein Skript in einer Jamf Pro Server Richtlinie festgelegt werden

Funktionen in Jamf Connect:

- Für den Anmeldebildschirm kann eine benutzerdefinierte Nachricht erstellt werden, die komplexe Kennwörter erzwingt, wie es die Cloud Identitätsrichtlinien vorschreiben

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen, um die Compliance für Systemzugriff, Authentifizierung und Autorisierung zu überprüfen

Weitere Überlegungen:

Mit Jamf Pro können IT-Administrator*innen zusätzliche Sicherheitseinstellungen anpassen, indem sie ein EFI-Kennwort festlegen, Wi-Fi in hochsicheren Umgebungen deaktivieren und vieles mehr. Sie können den Jamf Pro Server auch dazu verwenden, Ihre Macs umzubenennen, um die Bestandsaufnahme zu erleichtern. Darüber hinaus können Sie mit Jamf Pro eine Bestandsaufnahme der Software-Assets Ihrer Organisation durchführen und den Überblick über die Lizenzen behalten.

CIS-Benchmark-Empfehlungen:

- Drahtlose Technologie unter macOS
- Datenschutz und Vertraulichkeit beiiSight-Kameras
- Überlegungen zum Computernamen
- Überlegungen zum Softwarebestand
- Firewall-Betrachtung
- Automatische Aktionen für optische Medien
- App Store Automatisches Laden von Apps, die auf anderen Macs gekauft wurden Überlegungen
- Kennwort für die erweiterbare Firmware-Schnittstelle (EFI)
- FileVault und Lokales Konto Passwort zurücksetzen mit AppleID
- Berechtigungen müssen nicht mehr repariert werden
- App Store Passwort Einstellungen
- Siri auf macOS
- Funktionen der Apple Watch mit macOS
- Sicherung von Systeminformationen auf entfernten Computern
- Einheitliche Protokollierung
- AirDrop-Sicherheitsüberlegungen

Funktionen von Jamf Pro:

- Wi-Fi kann über das Konfigurationsprofildeaktiviert werden
- Die Benennung von Computern kann im Jamf Pro Serverautomatisiert werden
- Software-Bestand und Lizenzverfolgung auf dem Jamf Pro Server
- EFI-Passwörter können über eine Richtlinie festgelegt werden

Funktionen in Jamf Protect:

- Bewertet alle hier hervorgehobenen Einstellungen, um die Compliance zusätzlicher Überlegungen zu überprüfen

Schlussfolgerung

Jamf macht es einfach, den Benchmark des Center for Internet Security für macOS zu implementieren und zu befolgen.

jamf

www.jamf.com/de/

Testen Sie diese bewährten Sicherheitsverfahren mit einer kostenlosen Testversion von Jamf. **Los geht's.**