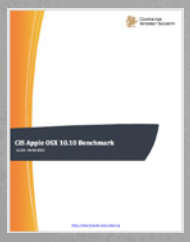


Checkliste zur Mac OS X-Sicherheit:

Implementieren des Center for Internet Security-Benchmarks für OS X

Empfehlungen zur Sicherung von Mac OS X

Der Center for Internet Security-(CIS-)Benchmark für OS X wird weitgehend als umfassende Checkliste betrachtet, mit der Unternehmen ihre Macs sichern können. In diesem White Paper von JAMF Software (den Experten im Management Ihrer Apple-Geräte) erfahren Sie, wie Sie die Empfehlungen der unabhängigen Organisation umsetzen.

Was ist die Casper Suite?

Die Casper Suite ist eine Reihe administrativer Tools zum Management Ihrer Apple-Geräte.

Was ist der JSS?

Der JAMF Software Server (JSS) ist die Managementserver-Komponente für die Suite, die auf einem Mac-, Windows- oder Linux-Server ausgeführt werden kann.

Was ist eine Policy?

Eine Policy ist das Hauptwerkzeug, mit dem Änderungen an einem Client-Mac implementiert werden. Der JSS sendet Befehle an einen Agent auf dem Mac.

Center for Internet Security®

Wer ist das CIS?

Das Center for Internet Security, Inc (CIS) ist eine gemeinnützige Organisation, die darauf abzielt, die Bereitschaft und Reaktionsfähigkeit von juristischen Personen im öffentlichen und privaten Sektor in Bezug auf Cybersicherheit zu verbessern.

So wurde der CIS-Benchmark aufgestellt

Der CIS-Benchmark wurde anhand eines Konsensprüfungsverfahrens unter Beteiligung von Fachexperten aufgestellt. Die Teilnehmer bieten Blickwinkel aus zahlreichen verschiedenen Hintergründen, wie Beratung, Softwareentwicklung, Audit und Compliance, Sicherheitsforschung, Geschäftsbetrieb, Regierungsbehörden und Rechtswesen.

Jeder CIS-Benchmark wird zwei Konsensprüfungsphasen unterzogen. Die erste Phase findet bei der anfänglichen Aufstellung des Benchmarks statt. In dieser Phase versammeln sich Fachexperten, um Arbeitsentwürfe des Benchmarks zu besprechen, zu erstellen und zu testen. Diese Besprechung wird so lange fortgesetzt, bis ein Konsens im Hinblick auf die Benchmarkempfehlungen erreicht wird. Die zweite Phase beginnt nach der Veröffentlichung des Benchmarks. In dieser Phase wird das gesamte Feedback von der Internet-Community vom Konsensteam in Bezug auf eine mögliche Einarbeitung in den Benchmark geprüft. Wenn Sie an einer Teilnahme am Konsensverfahren interessiert sind, gehen Sie zu https://community.cisecurity.org

- CIS-Benchmark für Apple OS X 10.10

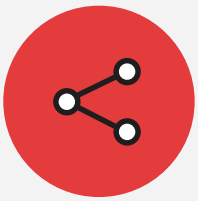
Sicherheitskategorien für OS X

Updates und Patches

Systemeinstellungen

iCloud

Protokollierung und Auditierung



Netzwerkkonfiguration

Benutzerkonten

Zugriff und Authentifizierung

Andere Aspekte

Installieren von Updates, Patches und Sicherheitssoftware

Mit der Casper Suite können Sie dafür sorgen, dass Ihr Betriebssystem und Ihre Anwendungen stets auf dem neuesten Stand sind, indem Sie Updates remote auf den Client-Macs verpacken und bereitstellen. Sie können sogar Berichte dazu erstellen, welche Rechner aktualisiert wurden und welche Updates noch ausstehen.

CIS-Empfehlungen:

- Per Software-Update-Tool sicherstellen, dass BS und Apps aktuell sind
- Automatische Updates in App Store aktivieren
- Automatische Sicherheitsupdates aktivieren

Features in der Casper Suite:

- Dank der Patch-Verwaltung in der Casper Suite können Sie Mac OS X auf dem neuesten Stand halten
- Mit einem benutzerdefinierten Softwareaktualisierungsserver können Sie genehmigte Updates für Ihre Macs zulassen
- Policy ausführen, um automatische Updates über den App Store zu aktivieren
- Policy ausführen, um nach Updates auf einem Client-Mac zu suchen

Systemeinstellungen

Mit der Casper Suite können Sie Systemeinstellungen entsprechend der Sicherheitsanforderungen Ihres Unternehmens konfigurieren. Häufig verwendete Einstellungen, wie Kennwörter und Bildschirmschoner, können einfach remote und als Massenvorgang aktiviert werden, um eingeschränkten physischen Zugriff auf Macs sicherzustellen. Erweiterte Einstellungen, wie Deaktivierung von SSH oder Dateifreigabe, können ebenfalls festgelegt werden, um den Mac vor Remote-Angriffen zu schützen.

CIS-Empfehlungen:

Bluetooth:

- Bluetooth deaktivieren
- Bluetooth-Sichtbarkeit deaktivieren

Datum und Uhrzeit:

- Automatische Einstellung von Datum und Uhrzeit aktivieren

Desktop und Bildschirmschoner:

- Bildschirmschoner auf höchstens 20 Minuten einstellen
- Aktive Ecken für Start des Bildschirmschoners aktivieren
- Ruhezustand für Monitor auf einen größeren Wert als Bildschirmschoner setzen

Freigabe:

- Remote-Apple-Ereignisse bei Freigabe deaktivieren
- Internetfreigabe deaktivieren
- Bildschirmfreigabe deaktivieren
- Druckerfreigabe deaktivieren
- Fernanmeldung (SSH) deaktivieren
- DVD- oder CD-Freigabe deaktivieren
- Bluetooth-Freigabe deaktivieren
- Dateifreigabe deaktivieren
- Fernverwaltung (ARD) deaktivieren

Energie sparen:

- „Ruhezustand bei Netzwerkzugriff beenden“ deaktivieren
- Ruhezustand des Computers bei Anschluss an Stromversorgung deaktivieren

Sicherheit:

- FileVault 2 aktivieren
- Gatekeeper aktivieren
- Firewall aktivieren
- Firewall-Tarnmodus aktivieren
- Programm-Firewall-Regeln prüfen (https://support.apple.com/de-de/HT201642)

Sonstiges:

- iCloud (siehe Abschnitt weiter unten)
- Sichere Tastatureingabe in terminal.app aktivieren
- Java 6 ist nicht die Standard-Java Runtime
- „Papierkorb sicher entleeren“ verwenden

Features in der Casper Suite:

- Alle der oben genannten Systemeinstellungen können über eine JSS-Policy und/oder ein Konfigurationsprofil festgelegt werden.
- FileVault 2 kann aktiviert werden, und Schlüssel können im JSS-Bestand hinterlegt werden.
- Bildschirmschoner- und Kennworteinstellungen können festgelegt werden.
- Freigabeeinstellungen können festgelegt werden.
- Sicherheitseinstellungen können festgelegt werden.
- Richtlinie zur Deaktivierung von Java kann implementiert werden.

iCloud und andere Cloud-Dienste

Die Casper Suite vereinfacht die Implementierung der iCloud-Strategie Ihres Unternehmens, da IT-Administratoren den Cloud-basierten Dienst blockieren oder aktivieren können.

CIS-Empfehlung:

„Apple iCloud ist nur eine der zahlreichen Cloud-basierten Lösungen für die plattformübergreifende Datensynchronisierung. Sie sollte konsistent mit anderen Cloud-Diensten in Ihrer Umgebung kontrolliert werden. Arbeiten Sie mit Ihren Mitarbeitern zusammen, und konfigurieren Sie den Zugriff so, dass die Daten am besten geschützt sind und das Ziel dennoch erreicht werden kann."

Features in der Casper Suite:

- iCloud kann über ein Konfigurationsprofil und/oder eine JSS-Richtlinie deaktiviert werden.
- Wenn iCloud nicht zugelassen ist, kann iCloud Drive aus dem Finder entfernt werden.

Protokollierung und Auditierung

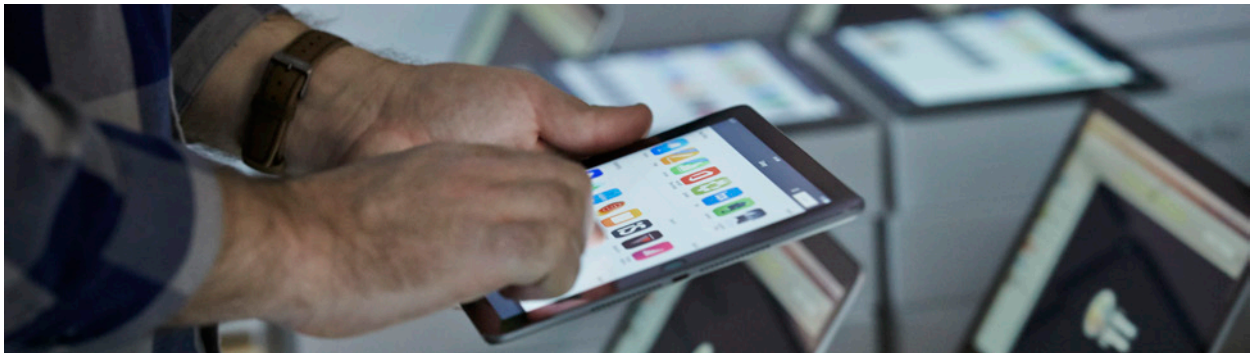
Mit der Casper Suite können IT-Administratoren die von OS X generierten Protokolle verfolgen und an einer zentralen Stelle aufbewahren. Administratoren können auch erweiterte Berichte zu diesen Protokollen ausführen, um nach potenziellen Sicherheitsproblemen zu suchen.

CIS-Empfehlung:

- asl.conf konfigurieren
- system.log mindestens 90 Tage lang beibehalten
- appfirewall.log mindestens 90 Tage lang beibehalten
- auth.log mindestens 90 Tage lang beibehalten
- Sicherheitsaudits aktivieren
- Sicherheitsauditkennzeichen konfigurieren
- Remote-Protokollierung für Macs in vertrauenswürdigen Netzwerken aktivieren
- install.log mindestens 1 Jahr lang beibehalten

Features in der Casper Suite:

- Konfigurationsdateien können mit einem Skript geändert werden.
- Protokolldateien können an den JSS gesendet und beliebig lange gespeichert werden.
- Weitere Protokolle können vom JSS im Cache abgelegt werden.



Netzwerkkonfigurationen

Die Casper Suite erleichtert die Einführung von Netzwerkkonfigurationen für IT-Administratoren, indem WLAN-, VPN- und sogar DNS-Einstellungen verteilt werden. Außerdem stellt die Casper Suite sicher, dass einige der älteren Serverkomponenten von OS X deaktiviert sind, sodass Benutzer nicht unabsichtlich ihnen unbekannte Ports öffnen.

CIS-Empfehlung:

- Sicherstellen, dass der WLAN-Status in der Menüleiste angezeigt wird
- Netzwerkspezifische Speicherorte erstellen
- Sicherstellen, dass der HTTP-Server nicht ausgeführt wird (Apache)
- Sicherstellen, dass der FTP-Server nicht ausgeführt wird
- Sicherstellen, dass der NFS-Server nicht ausgeführt wird

Features in der Casper Suite:

- Netzwerkeinstellungen können in ein Konfigurationsprofil integriert werden.
- Apache, FTP und NFS können allesamt über ein Skript in einer JSS-Richtlinie deaktiviert werden.

Benutzeraccounts und Umgebung

Dank der Casper Suite kann ein Unternehmen lokale Accounts in einem Mac verwalten, sodass Administratoren oder Standardbenutzer erstellt werden können. Die JAMF-Binärdatei in Clientrechnern erstellt einen verborgenen Managementaccount, der über Administratorrechte zum Ausführen von Befehlen und Erstellen neuer Benutzer verfügt. Sie können Richtlinien erstellen, um den Anmeldebildschirm weiter zu sichern und den Gastaccount zu deaktivieren.

CIS-Empfehlung:

- Anmeldefenster nur als Name und Kennwort anzeigen
- Anzeige von Kennworthinweisen deaktivieren
- Gastaccount deaktivieren
- Nicht zulassen, dass Gäste eine Verbindung mit freigegebenen Ordnern herstellen
- Dateinamenerweiterungen einschalten
- Automatische Ausführung sicherer Dateien in Safari für unterschiedliche Zwecke deaktivieren

Features in der Casper Suite:

- Anmeldefenster kann über ein Konfigurationsprofil konfiguriert werden.
- Gastaccount kann über eine JSS-Richtlinie deaktiviert werden.
- Benutzeraccounts können über Systemassistent und DEP (Programm zur Geräteregistrierung) oder Image-Erstellung erstellt werden.
- Accounts können je nach Bedarf als Standard- oder Administratoraccounts erstellt werden.

Systemzugriff, Authentifizierung und Autorisierung

Mit der Casper Suite können Sie Dateiberechtigungen festlegen, den Schlüsselbundzugriff verwalten und sichere Kennwortrichtlinien für Benutzer festlegen. Indem Sie ein Konfigurationsprofil oder eine JSS-Richtlinie erstellen, können Sie Systemzugriffseinstellungen remote aktivieren, um Ihre Macs besser zu schützen.

CIS-Empfehlung:

- Sicherer Benutzerordner (keine Leseberechtigungen für andere Benutzerordner erteilen)
- Berechtigungen regelmäßig reparieren
- Systemweite Anwendungen auf Berechtigungen prüfen
- Systemordner auf global beschreibbare Dateien prüfen
- Bibliotheksordner auf global beschreibbare Dateien prüfen
- Sudo-Zeitüberschreitung reduzieren
- Anmeldeschlüsselbund bei Inaktivität automatisch sperren
- Sicherstellen, dass der Anmeldeschlüsselbund gesperrt wird, wenn der Computer in den Ruhezustand übergeht
- OCSP- und CRL-Zertifikatsprüfung sicherstellen
- „root“-Account nicht aktivieren
- Automatische Anmeldung deaktivieren
- Kennwort anfordern, um den Ruhezustand des Computers zu beenden
- Administratorkennwort für den Zugriff auf systemweite Einstellungen anfordern
- Verhindern, dass Benutzer sich bei aktiven und gesperrten Sitzungen anderer Benutzer anmelden können
- Komplexe Kennwörter (mit Zahlen, Buchstaben und Symbolen)
- Mindestkennwortlänge festlegen
- Schwellenwert für Accountsperrung konfigurieren
- Benutzerdefinierte Nachricht für den Anmeldebildschirm erstellenCreate a login window banner
- Banner für Anmeldefenster erstellen
- Kennworthinweise deaktivieren
- Schnelle Benutzerumschaltung deaktivieren
- Individuelle Schlüsselbundelemente sichern
- Spezielle Schlüsselbunde für unterschiedliche Zwecke erstellen

Features in der Casper Suite:

- Ordnerberechtigungen können über ein Skript in einer JSS-Richtlinie festgelegt werden.
- Der Befehl zur Berechtigungsreparatur kann über den Self Service ausgelöst oder automatisch ausgeführt werden.
- Sie können Berichte erstellen, um in System und Bibliothek nach Dateien mit ungültigen Berechtigungen zu suchen.
- Kennwortrichtlinien können über ein Konfigurationsprofil aktiviert werden.
- Anmeldefenster und Banner können über eine JSS-Richtlinie hinzugefügt werden.

Weitere Aspekte

Mit der Casper Suite können IT-Administratoren zusätzliche Sicherheitseinstellungen anpassen, indem sie ein EFI-Kennwort festlegen, WLAN in besonders gesicherten Umgebungen deaktivieren und vieles mehr. Sie können Ihre Macs mit dem JSS auch umbenennen, um die Bestandsaufnahme zu vereinfachen. Darüber hinaus können Sie mit der Casper Suite einen Bestand der Software-Assets Ihres Unternehmens erstellen und Lizenzen verfolgen.

CIS-Empfehlung:

- Eventuell WLAN deaktivieren und nur Ethernet verwenden
- iSight-Kameras abdecken
- Computer mit logischen Namen versehen
- Bestand der Software erstellen
- Bestand der Software erstellen
- Firewall einsetzen
- Automatische Aktionen für optische Medien
- Automatische App Store-Downloads auf andere Macs deaktivieren
- EFI-Kennwort festlegen
- Rücksetzungen des Apple ID-Kennworts

Features in der Casper Suite:

- WLAN kann über ein Profil deaktiviert werden.
- Die Computerbenennung kann über eine Einstellung im JSS automatisiert werden.
- Softwarebestand und Lizenzverfolgung im JSS.
- EFI-Kennwörter können über eine Richtlinie und/oder Image-Erstellung festgelegt werden.

Fazit

Dank der Casper Suite ist es ein Einfaches, die Apple OS X-Benchmarks der unabhängigen Organisation Center for Internet Security umzusetzen und einzuhalten.

Weitere Informationen zur Sicherung Ihrer Macs mit der Casper Suite finden Sie unter **www.jamfsoftware.com/sichern-von-apple-geraten-mit-der-casper-suite**

JAMF software

germany@jamfsoftware.com | +49 699 675 97 37 | www.jamfsoftware.com/de