Apple Gerätesicherheit

FÜR BEGINNER

jamf

Ein gut geplanter Cyberangriff oder ein versehentlicher Download von Malware kann dafür sorgen, dass Ihre Arbeit lahmgelegt wird, wo Sie doch so produktiv hätten sein können. Da die Hacker*innen immer geschickter vorgehen, müssen Unternehmen, die sich um ihren Gewinn und die Sicherheit der Daten ihrer Nutzer*innen, wie Kund*innen, Mitarbeiter*innen oder Student*innen, sorgen, immer auf dem neuesten Stand der Sicherheit bleiben.

Apple Sicherheitsbedenken sind, wie alle IT-Sicherheitsbedenken, sehr real und stellen eine kritische Bedrohung für die Unternehmensressourcen und die Sicherheit der Beteiligten dar.

Apple stellt unglaublich sichere Betriebssysteme her. Es besteht kein Zweifel daran, dass die Konzentration auf die Sicherheit und den Schutz der Privatsphäre, die in die Hardware und Software integriert sind, eine wichtige Rolle bei der steigenden Beliebtheit und der massenhaften Akzeptanz in Unternehmen, Bildungseinrichtungen und anderen Branchenorganisationen gespielt hat. Und da Apple nach wie vor die bevorzugte Plattform für private und professionelle Hardware ist, ist sie ein attraktives Ziel für Angreifer*innen geworden. Dies bedeutet, dass Administrator*innen schnell auf Sicherheitsvorfälle reagieren müssen, sobald sie auftreten, und nicht warten dürfen, bis ein Problem auftritt. Stattdessen sind MacAdmins und Sicherheitsteams (und die von ihnen unterstützten Interessengruppen) besser beraten, sich proaktiv vor diesen Bedrohungen zu schützen, bevor sie sich zu etwas weitaus Schlimmerem entwickeln können, indem sie auf Apple zugeschnittene oder speziell für Apple entwickelte Lösungen einsetzen, um sich effektiv vor Apple zentrierten Bedrohungen zu schützen.

Dieser Leitfaden richtet sich an Administrator*innen und Manager*innen, die sich ernsthaft mit der organisatorischen Sicherheit ihrer Apple Geräte befassen wollen, und bietet grundlegende Informationen für Neulinge oder auch eine einfache Auffrischung für Apple Management-Veteran/innen.

Einführung in die Apple Sicherheit

Mehrere Faktoren wirken zusammen, um die Sicherheit der Hardware und Daten Ihres Unternehmens zu gewährleisten:

1. **Apple eigene Sicherheit:** Sicherheitssysteme, die bereits in macOS, iOS, iPadOS und tvOS integriert sind
2. **Registrierte Geräte:** Registrierung und Bereitstellung von Geräten mit sicherer, zentraler Verwaltung und Transparenz
3. **Sichern von Geräten:** Schützen Sie Ihre physischen Geräte und schützen Sie Ihre Benutzer*innen vor Bedrohungen
4. **Datenverschlüsselung:** Sicherung der Daten im Ruhezustand und bei der Übertragung, auf dem Gerät und im Netz zu jeder Zeit
5. **Überwachung der Einhaltung:** Überwachung von Geräten zur Bestimmung des Gesundheitszustands und zur Durchsetzung von Baselines
6. **Appsicherheit und Patching:** Immer auf dem neuesten Stand bei Betriebssystem-, App- und Software-Patches bleiben

1

BAUSTEIN EINS:

Apple Native Security

Apple Geräte sind die sichersten Hardware-Optionen auf dem Markt, und speziell entwickelte Verwaltungs- und Sicherheitslösungen erweitern die Leistungsfähigkeit von Apple.

Die bereits in macOS (dem Betriebssystem für Mac), iOS (dem Betriebssystem für iPad und iPhone) und tvOS (dem Betriebssystem für Apple TV) eingebauten Sicherheitsfunktionen sind umfangreich und bringen mehrere Vorteile mit sich:

- **Die Apple Betriebssysteme basieren auf UNIX, einer ausgereiften, gut erforschten Plattform mit tiefen Entwicklungswurzeln und felsenfester Stabilität.**
- **Starker OS Sicherheitsrahmen:**
  - Notarielle Beglaubigung
  - Gatekeeper
  - XProtect
  - Tool zum Entfernen von Malware (MRT)
  - Transparenz, Zustimmung und Kontrolle (TCC)
  - Schnelle Sicherheitsreaktionen
  - Abriegelungsmodus
- **Physische Gerätesicherheit in Form von Sperren und Verfolgung verlorener Geräte mit dem Find My Service**
- **Fähigkeit zur Implementierung und Konfiguration von Sicherheitskontrollen durch Konfigurationsoptionen über Mobile Device Management (Mobilgeräteverwaltung, MDM)**
  - Sichere Anmeldemodi sind in Apple Geräte integriert, wie z. B. die automatische Geräteanmeldung und die vom Benutzer/von der Benutzerin initiierte Anmeldung für unternehmenseigene und/oder persönliche Geräte, um alle Anforderungen an Eigentumsmodelle (wie BYOD, CYOD und COPE) ohne riskante Anmelde-URLs oder verdächtige E-Mail-Einladungen zu erfüllen
  - Nahtlose Integration mit Apple Business Manager oder Apple School Manager zur Unterstützung der zentralen Verwaltung der gesamten institutionellen Hardware, einschließlich der Überwachung von Geräten über die Luftschnittstelle und der sicheren Übergabe an Ihre MDM-Lösung für Geräteverwaltungsfunktionen, wie verwaltete App-Bereitstellung, sichere Gerätebereitstellung und Zero-Touch-Onboarding-Workflows

Eine speziell entwickelte MDM-Lösung kann diese bestehenden Sicherheitskonfigurationen übernehmen, sie an Ihre individuellen organisatorischen Anforderungen anpassen, einschließlich Branchen-Benchmarks, und sie für Ihre gesamte Apple Flotte bereitstellen (und auch durchsetzen), unabhängig von ihrer Größe. So können Sie einen Mac genauso sicher und effizient einrichten wie Tausende. Außerdem erhalten Sie umfassendere Sicherheitskontrollen mit einem MDM-Tool, das die Durchführung von Verwaltungsaufgaben auf allen von Ihnen ausgewählten Geräten erleichtert. So können Sie beispielsweise sich wiederholende Aufgaben schnell erledigen, indem Sie Geräte, die verloren gegangen sind oder aus dem Inventar Ihrer Einrichtung entfernt werden sollen, per Fernzugriff sperren und löschen. Weitere Informationen finden Sie in unserem E-Book Apple Geräteverwaltung für Einsteiger*innen.

Details zum Sicherheitsmerkmal

Native Sicherheitsfunktionen für macOS, iOS, iPadOS und tvOS

macOS	iOS und iPadOS	tvOS
Softwareaktualisierungen	Softwareaktualisierungen	Softwareaktualisierungen
Schutz der Systemintegrität (SIP)	Sicheres System	App Store
Gatekeeper	App Store	Airplay Einstellungen und Passwörter
App Store	Biometrische Identifizierung	App-Einschränkungen
FileVault Verschlüsselung	Hardwareverschlüsselung	Bildschirmschoner
Betreuung	Betreuung	Betreuung
XProtect und Malware Removal Tool (MRT)	App-Sandboxing	
Finden Sie mein	Finden Sie mein	
Datenschutz-Einstellungen	Datenschutz-Einstellungen	
Notarielle Beglaubigung und Aktenquarantäne	Sichere Enklave und biometrische Identifizierung	
Endpoint-Sicherheits-API	Notarielle Beglaubigung	
App-Sandboxing		
Sichere Enklave und biometrische Identifizierung		

2

BAUSTEIN ZWEI:

Sicher registrierte Geräte und Einsätze

Wie bei allen Bausteinen ist ein solides Fundament der Schlüssel zum Erfolg. Dieser informiert jeden nachfolgenden Baustein und gibt den übergreifenden Ton für das Management und die Sicherheit in Bezug auf die Lebenszyklen von Hardware und Apps an.

Der erste Schritt zur korrekten Bereitstellung von Geräten und ihrer sicheren, standardisierten und effizienten Verteilung in Ihrer gesamten Flotte ist die automatische Geräteanmeldung, die Teil der kostenlosen Dienste ist, die Apple über den Apple Business Manager und den Apple School Manager anbietet.

Mit der automatischen Geräteregistrierung können Sie Apple über alle Geräte informieren, die sich im Besitz Ihres Unternehmens befinden, sowie über andere Eigentumsmodelle, die weiter unten erläutert werden, und diese Geräte zur Verwaltung durch das MDM Ihres Unternehmens zuweisen. Wenn dann ein in diesem Programm registriertes Gerät eingeschaltet wird, wird es auch eingeschaltet:

- Automatische Anmeldung bei Ihrer MDM-Instanz
- Aktivieren Sie die Überwachung, die eine wesentliche Voraussetzung für strengere Sicherheitskontrollen ist
- Ermöglicht Administratoren die Anwendung von Konfigurationsprofilen und Härtungseinstellungen
- Sicherstellen, dass wichtige Sicherheitseinstellungen und Nutzdaten bereitgestellt werden, bevor der Benutzer/die Benutzerin ein Gerät verwenden kann
- Optimierte Verwaltung und Bereitstellung von Betriebssystem-Updates und Sicherheits-Patches
- Verringern Sie die Anzahl der Arbeitsabläufe für die Gerätebereitstellung, indem Sie die Beschaffung, Konfiguration und Bereitstellung von Apps zentralisieren, was auch die Sicherheit von Apps aus überprüften, vertrauenswürdigen Quellen gewährleistet
- Reduzieren Sie die Einrichtung von Geräten, indem Sie die Benutzer in die Lage versetzen, ihre Geräte ohne Unterstützung durch die IT-Abteilung zu warten
- Ermöglicht die Fernverwaltung unabhängig davon, welches unterstützte Gerät verwendet wird, von wo aus und über eine beliebige Netzwerkverbindung

Modelle zum Gerätebesitz

Die Automatisierung der Verwaltung und Sicherheit Ihrer Geräteflotte ist eine wichtige Funktion, insbesondere wenn die Anzahl der Geräte zunimmt und die Belegschaft dezentralisiert wird. Die zunehmende Akzeptanz und das Vertrauen in die Apple Plattform und mobile Geräte am Arbeitsplatz sind so vielfältig wie die Branchen und Nutzer*innen, die sich auf diese Geräte verlassen, um produktiv zu bleiben.

Einige Unternehmen haben sich Apple Produkte zu eigen gemacht, indem sie Mitarbeiterwahlprogramme eingeführt haben, die firmeneigene Geräte mit macOS und iOS und iPadOS zuweisen, während andere Unternehmen Apple am Arbeitsplatz einsetzen, indem sie ihren Mitarbeiter*innen erlauben, persönliche Geräte für den Zugriff auf Unternehmensressourcen zu nutzen. Indem sie ihnen die Möglichkeit geben, bequemer mit der Hardware und Software zu arbeiten, mit der sie am besten vertraut sind, können Unternehmen die Kosten für die Bereitstellung von Geräten für jeden Beteiligten einsparen - vor allem, wenn die Benutzer*innen bereits ein funktionales Gerät haben, das sie kennen und lieben.

Damit verschiebt sich die Frage von „Wie stellen wir die Geräte der Benutzer bereit?" zu „Wie stellen wir sicher, dass die Unternehmensressourcen geschützt bleiben?"

Hier treffen das MDM Ihres Unternehmens und flexible Geräteeigentumsmodelle aufeinander und bilden die Lösung für mehrere Geräteeigentumsmodelle, wie zum Beispiel:

Bring Your Own Device (BYOD)

Das wohl am weitesten verbreitete Modell, bei dem die Benutzer*innen ihre persönlichen Geräte für den Zugriff auf Unternehmensressourcen nutzen können. Wenn Benutzer*innen ihre Geräte manuell im MDM des Unternehmens registrieren müssen, bevor sie Zugang zu den Arbeitsressourcen erhalten, hat dies den doppelten Vorteil, dass die Benutzer sicher sein können, dass sie die erforderlichen Tools erhalten, um auf die Daten und Dienste zuzugreifen, die sie für die Erfüllung ihrer Arbeitsaufgaben benötigen, und dass die Unternehmen sicher sein können, dass die registrierten Geräte mit der erforderlichen Sicherheitssoftware und den erforderlichen Einstellungen ausgestattet sind, um die Geschäftsdaten während der Nutzung, im Ruhezustand und bei der Übertragung zu schützen.

Wählen Sie Ihr eigenes Gerät (CYOD)

Hierbei handelt es sich um eine Abwandlung des oben beschriebenen BYOD-Modells, mit dem Unterschied, dass das Unternehmen oder die Einrichtung häufig Eigentümer*innen der Geräte ist, die in diesem Modell verwendet werden und die für die Ausübung berufsbezogener Aufgaben oder zum Lernen (im Falle der Bildung) genutzt werden sollen. Jedes Gerät wird registriert, einem Stakeholder zugewiesen und durch das MDM des Unternehmens verwaltet. Die Apps, Konfigurationsprofile, Geräteeinstellungen und Sicherheitssoftware werden auf der Grundlage der Sicherheitslage des Unternehmens und unter Berücksichtigung der Arbeitsanforderungen des Mitarbeiters/der Mitarbeiterin bereitgestellt.

Firmeneigenes Personal (COPE)

Das COPE-Modell ist ein zunehmender Trend bei größeren Unternehmen, insbesondere bei solchen, die vollständig auf Fernarbeit umgestiegen sind oder ein hybrides Arbeitsumfeld haben. In diesem Fall kaufen und besitzen die Unternehmen die Geräte und registrieren und verwalten sie vollständig im MDM-System des Unternehmens. Wie bei CYOD werden die Tools, die die Beteiligten zur Erfüllung ihrer Aufgaben benötigen, je nach Gerät und Sicherheitslage des Unternehmens installiert und verwaltet. Ähnlich wie bei BYOD erlaubt die Organisation den Nutzer*innen jedoch, die Geräte neben der beruflichen Nutzung auch für den privaten Gebrauch zu verwenden, und ermutigt sie sogar dazu. Dadurch wird sichergestellt, dass die Unternehmensdaten innerhalb der verwalteten Apps und Konfigurationsprofile sicher bleiben. Dies kann dazu führen, dass Unternehmen über COPE-Geräte auf persönliche, private Daten zugreifen können. Es ist jedoch wichtig, den Schutz der Daten zu berücksichtigen und für die richtige Verwaltung und den Schutz der Daten auf diesen Geräten zu sorgen, und zwar mit Hilfe von Acceptable Use Policies (AUPs) und Datenmanagement.

Flexible Einschreibemethoden

Um die Verwaltung mehrerer Gerätebesitzmodelle innerhalb derselben MDM-Umgebung zu vereinfachen, hat Apple zwei verschiedene Registrierungsmethoden entwickelt, die in Verbindung miteinander verwendet werden, um die organisatorische Sicherheit zu verwalten und durchzusetzen, ohne die Privatsphäre der Benutzer*innen zu beeinträchtigen und umgekehrt.

Automatisierte Geräteregistrierung
Dies ist die gängigste Methode, für die sich die meisten Unternehmen mit unternehmenseigenen Geräten entscheiden. Diese Methode bescheinigt, dass jeder Schritt in der Registrierungskette verifiziert ist: von der Beschaffung bei Apple (oder einem autorisierten Drittanbieter*innen) über die Voreinstellung im MDM bis hin zur Registrierungsphase, die mit dem Einschalten des Geräts beginnt - jeder Schritt erfolgt in einem automatisierten Verfahren von Apple über das MDM zum Administrator/zur Administratorin für die laufende Verwaltung. Da diese Kette verifiziert ist, wird Supervision auf Geräten aktiviert, die über Automated Device Enrollment registriert werden. Dies dient als vertrauenswürdige Grundlage, die es der IT-Abteilung ermöglicht, die volle Kontrolle über das Gerät während seines gesamten Lebenszyklus zu erhalten. Die Überwachung ist die Wurzel des Vertrauens, die für die Durchführung bestimmter Verwaltungsaufgaben auf verwalteten Geräten erforderlich ist.

Benutzerinitiierte Geräteregistrierung
Diese Anmeldemethode ist neuer und häufiger, wenn die angemeldeten Geräte im Rahmen eines BYOD-Modells im persönlichen Besitz sind. Bei der automatischen Geräteanmeldung muss der Benutzer/die Benutzerin oder Eigentümer des Geräts sein Gerät manuell in der App „Einstellungen" anmelden und sich mit seinen Unternehmensdaten authentifizieren. Nach Abschluss der Benutzerregistrierung stellt das MDM des Unternehmens eine sichere Zwei-Wege-Kommunikation zwischen dem Gerät des Benutzers/der Benutzerin und der Verwaltungslösung des Unternehmens her.

Administrator*innen können verwaltete Apps installieren, Konfigurationsprofile bereitstellen und bestimmte Einstellungen ändern, indem sie eine Reihe von Konfigurationen verwenden, die es Unternehmen ermöglichen, gerätespezifische Anforderungen festzulegen und Verwaltungsaktionen oder -anforderungen mit dem Benutzer/der Benutzerin und nicht mit dem gesamten Gerät zu verknüpfen. Apple hat die Einschränkung so konzipiert, dass Unternehmen die notwendigen Schritte unternehmen können, um den Zugriff auf ihre Daten, die Interaktion mit Apps, die Speicherung auf dem Gerät und die Übertragung über Netzwerke zu sichern, ohne die persönlichen Apps, Daten und privaten Informationen auf dem Gerät zu beeinträchtigen. Unternehmen können die Sichtbarkeit von verwalteten Geräten anpassen, indem sie eine persönliche Apple ID mit persönlichen Daten und eine verwaltete Apple ID mit Unternehmensdaten verknüpfen.

3

BAUSTEIN DREI:

Sicherung von Geräten

Schutz von Geräten, Daten und Nutzer*innen vor Bedrohungen

„Hacker müssen es nur einmal richtig machen, wir müssen es jedes Mal richtig machen."

- Chris Triolo, HP

Wenn wir auf einige der größten, komplexesten und sogar tödlichsten Datenschutzverletzungen der jüngeren Geschichte zurückblicken, werden wir eine Gemeinsamkeit feststellen. Angriffe wie Stuxnet legten das iranische Atomanreicherungsprogramm lahm, indem sie den Laptop eines Auftragnehmers/einer Auftragnehmerin infizierten, der die SCADA-Anlagen aktualisierte. LinkedIn wurde von einem Entwickler/einer Entwicklerin ins Visier genommen, der die API des Unternehmens ausnutzte, um die persönlichen Daten von 700 Millionen Nutzer*innen abzugreifen und die Daten online zu verkaufen. Aadhaar - die größte ID-Datenbank, einschließlich personenbezogener und finanzieller Daten, für mehr als 1,1 Milliarden indische Bürger - wurde von Bedrohungsakteur*innen gestohlen und verkauft, nachdem sie sich über eine ungeschützte, mit der Datenbank verbundene Website Zugang verschafft hatten. In diesen und ähnlichen Fällen wurden die Angriffe durch das Anvisieren und Kompromittieren eines einzigen Geräts ermöglicht.

Eine der häufigsten Möglichkeiten, die Sicherheitsvorkehrungen eines Unternehmens zu umgehen und sich Zugang zu sensiblen Daten zu verschaffen und gleichzeitig die Sicherheit der Endbenutzer*innen zu gefährden, ist die Kompromittierung eines einzelnen Geräts. Unabhängig davon, in welcher Branche Ihr Unternehmen tätig ist oder ob es Daten und/oder Ressourcen für Wissensarbeiter*innen, Student*innen, Lehrer*innen, Gesundheitsdienstleister*innen, Außendienstmitarbeiter*innen, Einzelhandelsmitarbeiter*innen oder Vielreisende bereitstellt - zu jedem beliebigen Zeitpunkt können sich Ihre Geräte an jedem beliebigen Ort der Welt befinden und über eine beliebige Anzahl von nicht vertrauenswürdigen Netzwerken verbunden sein, was das Risiko von Bedrohungen sowohl für das Gerät als auch für das Unternehmensnetzwerk exponentiell erhöht.

Verlorene oder gestohlene Geräte

Ein verlorenes oder gestohlenes iPhone, iPad oder Mac ist nicht nur ein finanzieller Verlust: Es stellt auch ein massives Sicherheitsrisiko dar, dessen Auswirkungen unabsehbar sein können. Die folgenden Beispiele verdeutlichen, wie wichtig es ist, das Risiko für verlorene und gestohlene Geräte zu mindern:

SZENARIEN DER REALEN WELT

Ein externer Mitarbeiter/eine externe Mitarbeiterin bereitet juristische Dokumente für einen laufenden Haftungsfall vor, der vor Gericht verhandelt wird, und arbeitet von einem nahe gelegenen Café aus. Sie lassen den firmeneigenen Mac Laptop kurz unbeaufsichtigt, während sie ihren Kaffee nachfüllen, und genau in diesem Moment kommt ein Dieb herein und stiehlt den Laptop. Wenn das Gerät entsperrt ist, hat der Angreifer ungehinderten Zugang zu sensiblen und möglicherweise vertraulichen Unternehmensdaten, die sich negativ auf laufende Gerichtsverfahren und den Ruf des Unternehmens auswirken könnten.

In einem zweiten Beispiel verlegt ein Schüler, der sein persönliches iPhone benutzt, um über das Bildungsportal auf schulbezogene Ressourcen zuzugreifen, sein Gerät, während er die Klasse wechselt. Ein anderer Benutzer/eine andere Benutzerin findet das Telefon und greift auf die Kontodaten des Schülers/der Schülerin zu, wodurch er Zugang zu sensiblen personenbezogenen Daten wie Adresse, Telefonnummer oder Studentenausweis erhält. Ein unbefugter Benutzer/eine unbefugte Benutzerin kann solche PII-Informationen zum Identitätsdiebstahl oder zur Begehung von Straftaten nutzen, indem er sich als das Opfer ausgibt. Das Gerät kann sogar mit Malware kompromittiert und an das Opfer zurückgegeben werden, wodurch dessen Sicherheit und Wohlbefinden durch Fernverfolgung und Stalking durch Bedrohungsakteur*innen gefährdet wird.

Einfach gesagt: Geräte gehen verloren und werden gestohlen. Unfälle und Momente der Unachtsamkeit kommen vor. Dennoch ist die Planung - in der Annahme, dass es nur eine Frage der Zeit ist, wann und nicht ob jemand ein Gerät aus den Augen verliert - ein entscheidender Schlüssel, um sicherzustellen, dass die richtigen Strategien zur Risikominimierung vorhanden sind, bevor Geräte verloren gehen oder gestohlen werden.

Weitere Überlegungen zur Benutzer- und Datensicherheit sind, dass viele Geräte - insbesondere solche für Student*innen und Patient*innen oder gemeinsam genutzte Geräteumgebungen für mehrere Benutzer*innen - Schutzmaßnahmen gegen Missbrauch, die versehentliche Entdeckung fremder Daten oder den Zugriff auf und die Anzeige von riskanten und unangemessenen Inhalten erfordern.

Abhängig von den individuellen Anforderungen Ihres Unternehmens kann die Härtung von Sicherheitseinstellungen und die Konfiguration von Geräten, die mit den Unternehmens- und Compliance-Anforderungen übereinstimmen, ein beträchtliches Unterfangen sein, das zeit- und arbeitsintensiv ist, insbesondere wenn die Anzahl der Geräte steigt.

Wenn Sie Geräte manuell sichern oder einschränken, müssen Sie dies tun:

Mac

- Verlangt Passwörter für alle Geräte
- Aktivieren Sie „Meinen Mac suchen” über Systemeinstellungen>iCloud
- Abhängig davon, dass sich die einzelnen Benutzer*innen bei iCloud anmelden oder sich an ihr Passwort erinnern können (Voraussetzung für die Aktivierung von FindMy)
- Meldung an Apple, wenn ein Gerät verloren oder gestohlen wurde, wobei die Möglichkeit besteht, das Löschen zu veranlassen
- Verfolgen Sie das gesamte Inventar anhand von Mac Seriennummern oder Asset-Tags
- Aktivieren Sie die Kindersicherung auf dem Gerät, um ungeeignete Inhalte und bösartige Websites zu blockieren (mit dem Safari-Browser)
- Macs mit allen System- und Programm-Updates auf dem neuesten Stand halten, um Schwachstellen zu minimieren
- Konfigurieren und Härten von Geräteeinstellungen, um Fehlkonfigurationen zu minimieren, die Daten ungesichert lassen könnten
- Unterstützte Apps bereitstellen und auf dem neuesten Stand halten
- Installation und Konfiguration von Endpoint-Sicherheit zur Überwachung von Geräten, Erkennung und Beseitigung von Bedrohungen

Telefon und iPad

- Verlangt Passwörter für alle Geräte
- Aktivieren Sie „Meinen Mac suchen” über Systemeinstellungen>iCloud
- Es hängt von den einzelnen Nutzer*innen ab, ob sie sich bei iCloud anmelden oder ihr Passwort behalten können
- Nachverfolgung des gesamten Inventars anhand von Geräteseriennummern oder Asset-Tags
- Meldung an Apple, wenn ein Gerät verloren oder gestohlen wurde, wobei die Möglichkeit besteht, das Löschen zu veranlassen
- Aktivieren Sie die Kindersicherung für ein einzelnes Gerät und erstellen Sie für jedes Gerät ein eigenes Konto
- Halten Sie iOS basierte Geräte mit allen System- und App-Updates auf dem neuesten Stand, um Schwachstellen zu minimieren
- Konfigurieren und Härten von Geräteeinstellungen, um Fehlkonfigurationen zu minimieren, die Daten ungesichert lassen könnten
- Verwaltete Appsn bereitstellen und auf dem neuesten Stand halten
- Installieren Sie Endpoint-Sicherheit, um Geräte zu überwachen, Bedrohungen zu erkennen und zu beseitigen

Apple TV

- Passwörter auf allen Apple TVs erforderlich machen
- Einschränkungen konfigurieren
  - Gehen Sie im Hauptmenü zu Einstellungen > Allgemein > Einschränkungen
  - Wählen Sie Beschränkungen, um sie zu aktivieren
  - Geben Sie nach Aufforderung einen vierstelligen Passcode ein
  - Geben Sie die vier Ziffern zur Bestätigung erneut ein und wählen Sie dann OK
  - Merken Sie sich den Passcode
  - Wiederholen Sie den Vorgang für alle Apple TVs

So schränken Sie Airplay für Apple TV ein:

- Gehen Sie im Hauptmenü zu Einstellungen > AirPlay auswählen
- AirPlay ein- oder ausschalten

Wählen Sie aus:

- Alle
- Jeder im selben Netzwerk
- Wiederholen Sie den Vorgang für alle Apple TVs

Bei einer Best-of-Breed-MDM-Lösung wie Jamf Pro werden dieselben Verwaltungsaufgaben wie oben beschrieben ausgeführt, um Geräte zu sichern oder einzuschränken, und zwar folgendermaßen

Mac, iPhone, iPad und Apple TV

- Legen Sie alle Einschränkungen und Sicherheitsfunktionen ab der ersten Verwendung fest oder aktivieren Sie sie automatisch mit Supervision und vertrauenswürdigen Konfigurationsprofilen und Richtlinien
- Sperren oder Löschen eines verlorenen oder missbräuchlich genutzten Geräts aus der Ferne, unabhängig von seinem physischen Standort - und unabhängig davon, ob das Gerät mit einem iCloud-Konto angemeldet ist oder nicht (keine Apple ID erforderlich)
- Ermöglichen Sie mehreren Nutzer*innen die sichere gemeinsame Nutzung von Geräten, indem Sie ein Gerät zwischen den Nutzungen löschen und den Nutzer*innen erlauben, ihre Anmeldedaten und Einstellungen zu verwenden, die mit dem Nutzer/der Nutzerin verbunden sind - nicht mit dem Gerät
- Konfigurieren Sie verwaltete Apple IDs, die dem Gerät für geschäftliche Aufgaben zugewiesen werden, während der Benutzer/die Benutzeri mit seiner privaten Apple ID auf persönliche Apps, Daten und Einstellungen zugreifen kann, die in iCloud gespeichert sind
- Inventarisierung aller Geräte, einschließlich der Möglichkeit, sie nach einer beliebigen Kategorie zu gruppieren - nicht nur nach Seriennummer oder Asset-Tag -, um alle erforderlichen Daten zu erfassen, z. B. Benutzerzuweisungen, Betriebssystemversion oder installierte Apps, um nur einige zu nennen
- Durchführung von Verwaltungsaufgaben, bei denen Befehle an ein einzelnes Gerät oder in großen Mengen ausgegeben werden, z. B. die Bereitstellung von Sicherheitsupdates, die Aktualisierung auf eine neue Betriebssystemversion oder die administrative Löschung vergessener Passwörter auf gesperrten Geräten
- Implementieren Sie Kindersicherungen und blockieren Sie den Zugriff auf riskante oder ungeeignete Apps, indem Sie granulare Beschränkungen auf der Grundlage bestimmter Kriterien oder für alle Geräte auf einmal anwenden
- Stellen Sie verwaltete Apps bereit, die Benutzer benötigen, um zu Hause, im Büro, in der Schule oder anderswo produktiv zu sein. Vorabgenehmigung von Apps, die in der Self-Service-App gehostet werden sollen, damit die Nutzer*innen genau dann auf die Software zugreifen können, wenn sie sie brauchen
- Integrieren Sie Endpunktsicherheitslösungen in Ihr MDM, um sicherzustellen, dass Geräte ständig überwacht und vor Sicherheitsbedrohungen geschützt werden, und geben Sie gleichzeitig umfangreiche Telemetriedaten an das MDM weiter, um ein richtlinienbasiertes Management zur Automatisierung der Reaktion auf Vorfälle zu ermöglichen
- Verwalten Sie jede Facette der Geräteverwaltungsaufgaben zentral, um sicherzustellen, dass Geräte, Benutzer*innen und Daten vor Cyber-Bedrohungen geschützt sind und die Privatsphäre der Benutzer*innen gewahrt bleibt

Diese Erfahrung erleichtert nicht nur die Arbeit der IT-Administrator*innen und -Mitarbeiter*innen, sondern unterstützt auch die Endbenutzer*innen. Es bietet das Erlebnis, das die Menschen lieben und von Apple erwarten, ohne dass organisatorische, branchenspezifische und sicherheitsrelevante Anforderungen oder die Privatsphäre der Nutzer*innen zugunsten strengerer Sicherheitskontrollen geopfert werden.

4

BAUSTEIN VIER:

Daten verschlüsseln

Die Grundlagen von Daten im Ruhezustand und Daten bei der Übertragung und wie man beide Arten von Daten sicher hält.

Ganz gleich, ob es sich bei Ihrer Organisation um eine Schule zum Schutz von Schülerdaten, eine Einrichtung des Gesundheitswesens zum Schutz der Gesundheitsdaten von Patient*innen oder um ein Unternehmen zum Schutz Ihres geistigen Eigentums handelt, Verschlüsselung ist für Ihr Unternehmen keine Option mehr: Sie ist eine wichtige Voraussetzung für jedes Unternehmen, das sensible, vertrauliche und unternehmenskritische Daten oder wirklich Daten jeglicher Klassifizierung schützen möchte.

Nachfolgend finden Sie eine Zusammenfassung der drei Zustände der Daten zu einem bestimmten Zeitpunkt auf einem Gerät:

Daten im Ruhezustand: lokal (in der Regel) auf einem Gerät gespeichert, auf das gerade nicht zugegriffen wird oder das nicht genutzt wird.

Daten in Bewegung: Über einen Kommunikationskanal, z. B. ein drahtgebundenes oder drahtloses Netz, übertragene Daten, die sowohl empfangen als auch gesendet werden.

Verwendete Daten: Daten, die weder dauerhaft gespeichert noch über Netze übertragen werden, d. h. Daten, die gerade von Apps oder anderen Prozessen bearbeitet werden.

Jeder Staat birgt seine eigenen Risiken, was bedeutet, dass eine Lösung für einen Staat im Allgemeinen nicht in vollem Umfang für einen anderen Staat kompensiert werden kann (oder überhaupt nicht funktioniert). Dies erhöht zwar die Komplexität Ihrer Sicherheitsstrategie, aber keine Sorge, denn effektive Lösungen basieren alle auf der grundlegenden Funktion der Verschlüsselung.

SZENARIEN DER REALEN WELT

Ein neuer Mitarbeiter/eine neue Mitar eiterin in der Personalabteilung Ihres Unternehmens erhält seinen neuen Mac und schließt den Einrichtungsprozess schnell ab, um mit der Arbeit zu beginnen. Eine ihrer Aufgaben besteht darin, **mithilfe einer Tabellenkalkulationssoftware** eine Kontaktliste für Notfälle zu erstellen, die den Namen, die Berufsbezeichnung, die E-Mail-Adresse des Unternehmens, die persönliche Adresse und die persönliche Kontaktnummer jedes Mitarbeiters enthält und angibt, ob es sich um einen Haupt- oder einen Ersatzkontakt handelt. Diese Informationen müssen lokal auf dem Computer **gesichert** werden, einschließlich der persönlichen Kontaktinformationen für Mitglieder des Managements und der C-Suite-Teams, und autorisierten Stakeholdern muss ein Duplikat zur Verfügung gestellt werden, damit sie **von einem Cloud-Repository aus sicher darauf zugreifen können.**

Im obigen Szenario zeigen die fettgedruckten Abschnitte ein spezifisches Beispiel für jeden Datenzustand. Zunächst einmal ist die „Verwendung von Tabellenkalkulationssoftware" ein Beispiel für Daten in Verwendung, was bedeutet, dass die Daten sicher bleiben müssen, während sie in der App bearbeitet werden. Dies erfordert, dass die Integrität der Software überprüft und verifiziert wird, um sicherzustellen, dass ein Angreifer/eine Angreiferin oder bösartiger Code die interne Sicherheit nicht beeinträchtigt hat. Zweitens ist „lokal gesichert" ein Beispiel für ruhende Daten, was darauf hinweist, wie wichtig die Verschlüsselung ist, um zu verhindern, dass Unbefugte auf die Daten zugreifen und sie lesen können. Drittens ist der „sichere Zugriff von einem Cloud-Speicher" ein Beispiel für Daten in Bewegung, d. h. für Daten, die über eine Netzverbindung gesendet und empfangen werden. Die für die Kommunikation verwendeten Netzwerkverbindungen müssen Ende-zu-Ende verschlüsselt werden, um sicherzustellen, dass nur die beiden Verbindungen an beiden Enden die Nachricht erfolgreich entschlüsseln können und diese Daten vor unbefugtem Empfang oder Lauschangriffen schützen.

Da Zero Trust Network Access (ZTNA) eine Verschlüsselung für Daten in Bewegung bietet, integriert sich ZTNA auch mit Ihrem Identitätsanbieter (IdP) und stellt sicher, dass nur Benutzer*innen und Geräte, die sich erfolgreich authentifiziert haben und über die erforderlichen Zugriffsrechte verfügen, Zugang zu den angeforderten Ressourcen hinter zusätzlichen Schutzschichten erhalten, wobei das Prinzip der geringsten Rechte gewahrt bleibt. Im Gegensatz zu herkömmlichen VPN-Diensten, die nach der Authentifizierung oft Zugriff auf das gesamte Netzwerk gewähren, nutzt die ZTNA-Implementierung zur Sicherung von Verbindungen Mikrotunnel, um für jede geschützte App oder jeden geschützten Dienst einen eigenen Tunnel aufzubauen. Dies sorgt für mehr Sicherheit, indem das Prinzip der geringsten Privilegien durchgesetzt wird und gleichzeitig Gesundheitsprüfungen eingesetzt werden, um sicherzustellen, dass die Geräte - in Verbindung mit den Anforderungen für die Benutzerauthentifizierung - bei jeder Anfrage und vor der Gewährung des Zugangs Mindestanforderungen erfüllen.

Wie verschlüsselt man die drei Zustände von Daten?

Daten im Ruhezustand

Volumen- oder vollständige Geräteverschlüsselung

Die Verschlüsselung von Daten, die auf einem mobilen Gerät oder auf einem Datenträger auf Ihrem Computer gespeichert sind, ist aus mehreren Gründen eine bewährte Praxis. Der einfach zu konfigurierende Prozess zur Aktivierung der Verschlüsselung besteht aus proaktiven und reaktiven Maßnahmen und bietet ein Höchstmaß an Sicherheit für ruhende Daten in der permanenten Speicherung. Durch die Verwendung von Algorithmen, für die Angreifer*innen Hunderte oder wahrscheinlich Tausende von Jahren rund um die Uhr mit den leistungsfähigsten Computern arbeiten müssten, um sie zu überwinden, ist es ein „no brainer", wenn es darum geht, diese Sicherheitskontrolle als Teil einer Defense-in-Depth-Strategie einzubeziehen - wie The Alamo oder das sprichwörtliche letzte „Gefecht" zwischen einem Bedrohungsakteur*innen und vertraulichen Daten.

Nehmen Sie zum Beispiel einige häufige Sicherheitsvorfälle, die durch die Aktivierung der vollständigen Geräte- oder Datenträgerverschlüsselung wirksam gemildert werden können:

Verlust oder Diebstahl eines Geräts

Verlegte Geräte wie iPhones, iPads oder MacBook Laptops sind bei mobilen Geräten besonders häufig. Je größer die Mobilität, desto größer das Risiko von Verlust oder Diebstahl. Sobald ein Gerät nicht mehr in Ihren Händen ist, haben Bedrohungsakteur*innen jedoch freie Hand, um an die auf dem Gerät gespeicherten Daten zu gelangen.

Sicher, ein komplexer Passcode oder ein sicheres Passwort sollte Ihr Gerät schützen. Je nach Gerät gibt es jedoch immer noch alternative Möglichkeiten für Angreifer*innen, auf einige oder alle auf dem Gerät enthaltenen Daten zuzugreifen - es sei denn, sie sind verschlüsselt. Durch die einfache Aktivierung der Verschlüsselung werden die Daten so verschlüsselt, dass sie nicht mehr lesbar sind, es sei denn, der Entschlüsselungsschlüssel entschlüsselt sie. Es spielt keine Rolle, ob das Gerät zum Anmeldebildschirm gebootet wird oder ob auf die SSD irgendwie zugegriffen wird und sie als externes Laufwerk mit einem anderen Gerät verbunden ist. Verschlüsselte Daten bleiben so lange verschlüsselt, bis sie mit dem Entschlüsselungs- oder Wiederherstellungsschlüssel entschlüsselt werden - in jedem anderen Fall werden die Daten unlesbar und damit unbrauchbar.

Physischer Zugang

Ähnlich wie beim Abschnitt über verlorene oder gestohlene Geräte bedeutet der physische Zugriff auf ein Gerät nicht, dass es zuerst verlegt werden muss. Denken Sie an ein gemeinsam genutztes Gerät in einem Arbeitsbereich, vielleicht den Ihnen zugewiesenen Computer an Ihrem Schreibtisch oder ein anderes Computergerät, das ein Bedrohungsakteur möglicherweise unbemerkt zu nutzen versucht. Wenn Ihre Sitzung beendet ist und Sie sich abmelden, Ihr Gerät herunterfahren oder sogar sperren, während Sie weggehen oder es nicht benutzen, sind und bleiben die auf dem Volume oder Gerät enthaltenen Daten verschlüsselt. Zur Entschlüsselung der Daten ist ein Entschlüsselungs- oder Wiederherstellungsschlüssel erforderlich, um lesbaren Zugriff auf die gesicherten Daten zu erhalten.

Einhaltung von Vorschriften

Je nachdem, welcher Branche Ihr Unternehmen angehört, unterliegen Sie möglicherweise Gesetzen - sogenannten Vorschriften -, die Mindestanforderungen für den Schutz von Daten und deren Verarbeitung regeln und auch Beschränkungen dafür vorschreiben, welche Stellen mit geschützten Datentypen arbeiten dürfen. Bestimmte Branchen sind stärker reguliert als andere; dies sind stark regulierte Branchen wie der Finanzsektor und das Gesundheitswesen, während andere sich nur auf bestimmte Aspekte der Datensicherheit konzentrieren, wie z. B. Bildungsvorschriften, die das Wohlergehen von Schüler*innen und Student*innen und die mit ihnen verbundenen personenbezogenen Daten schützen sollen.

Wie bereits erwähnt, basieren Verordnungen auf Gesetzen, und ein Verstoß gegen sie könnte schwerwiegende Folgen für die Organisation oder Einrichtung haben, wenn sie sich nicht ordnungsgemäß an die Regeln der leitenden Organe gehalten hat. Oft ist die Verschlüsselung von Daten eine Sicherheitskontrolle, die während verschiedener Datenzustände erforderlich ist , z. B. im Ruhezustand oder in Bewegung, um das Risiko zu minimieren, dass regulierte Informationen durch Datenlecks, Exfiltration oder sogar Exposition gegenüber unbefugten Benutzern in die falschen Hände geraten.

Datenverschlüsselung und Apple Geräte

- macOS hat mit FileVault bereits eine integrierte Volume-Verschlüsselung. Sie müssen keine zusätzliche Software hinzufügen, um einen Ordner, eine Festplatte oder ein Volume auf einem Mac zu verschlüsseln.
- Neuere Macs, wie die von Apple Silicon, nutzen die sichere Enklave. Eine spezielle Hardwarekomponente, die für die Erstellung und Speicherung von Verschlüsselungsschlüsseln zuständig ist und auch algorithmische Berechnungen durchführt.
- Intel-basierte Macs verwenden eine ähnliche spezielle Hardwarekomponente, den T2-Sicherheitschip, der ähnliche Funktionen wie die sichere Enklave bietet.
- FileVault ist nach FIPS 140-2 zertifiziert. Das bedeutet, dass das Verschlüsselungssystem von Apple zertifiziert ist und die höchsten Standards für die Verschlüsselung durch die Bundesregierung erfüllt.
- Sie können FileVault manuell oder per Fernzugriff aktivieren: Einzelne Benutzer können die Option auf einem Gerät wählen, oder die IT-Abteilung kann die Aktivierung (mit Jamf Pro) automatisieren und auf Hunderten oder sogar Tausenden von Geräten mit einer Richtlinie durchsetzen.
- Gewähren Sie Nutzer*innen Zugriff auf verschlüsselte/entschlüsselte Volumes, indem Sie sich einfach bei macOS authentifizieren oder ihren Passcode auf iOS und iPadOS Geräten eingeben. Benutzer von unterstützten Geräten können die TouchID- oder FaceID-Technologien von Apple nutzen, um eine zusätzliche Sicherheitsebene für den Datenschutz zu schaffen, indem sie entweder ihren Fingerabdruck oder ihre Gesichtserkennungsmuster verwenden.

So aktivieren Sie FileVault manuell unter macOS:

- Navigieren Sie zu Systemeinstellungen > Datenschutz und Sicherheit > FileVault
- Wählen Sie die Schaltfläche „Einschalten...", um die Volumenverschlüsselung zu aktivieren
- Wiederholen Sie den Vorgang für alle Geräte

Um FileVault für alle Geräte in Ihrem Unternehmen zu aktivieren, nutzen Sie Ihre MDM Lösung, um die Verschlüsselung zu automatisieren, bereitzustellen und durchzusetzen. Sie können ein Konfigurationsprofil oder eine Richtlinie bereitstellen, um FileVault zu aktivieren. Die IT-Abteilung kann die Wiederherstellungsschlüssel abrufen, falls die Mitarbeiter*innen das Volume später entschlüsseln müssen.

- Erstellen Sie ein Konfigurationsprofil durch eine einfache Auswahl von Optionen in Jamf Pro
- Granulare Bereitstellung auf beliebig vielen Geräten oder auf allen macOS basierten Geräten
- **Es gibt keinen dritten Schritt**

Mit Jamf Pro können Sie auch die Umleitung des Wiederherstellungsschlüssels konfigurieren - selbst wenn der Benutzer FileVault selbst aktiviert. Die IT-Abteilung hat dann den Schlüssel in ihrer Verwaltungslösung gespeichert, um ihn leicht über die Geräteaufzeichnungen abrufen zu können.

Wie wäre es mit einem iPad oder iPhone?

Die Verschlüsselung von iOS und iPadOS Geräten ist sogar noch einfacher. iOS basierte Geräte verfügen über eine integrierte Verschlüsselung, die aktiviert wird, sobald ein Passcode festgelegt wird. Sie können dies individuell tun oder von Jamf Pro verlangen, ebenso wie die Einstellung der Parameter für die Stärke des Passcodes, wie z. B. Mindestlänge und Komplexitätsanforderungen.

Daten im Transit

Verschlüsselung von Netzwerkverbindungen von Ende zu Ende

Herkömmliche bewährte Verfahren schreiben die Verwendung eines VPN vor, um Daten bei der Übertragung von einem Gerät zu einem anderen Dienst zu schützen. Diese Methode reicht Jahrzehnte zurück und wurde zu einer Zeit entwickelt, als VPNs dazu dienten, zwei unterschiedliche Netzwerke sicher über ein nicht vertrauenswürdiges Netzwerk wie das Internet zu verbinden.

Und obwohl diese Sicherheitskontrolle von vielen Privat- und Unternehmensanwendern nach wie vor aktiv genutzt wird, haben die Veränderungen in der Computerlandschaft in den letzten Jahren, die sich aus der Einführung von Apple am Arbeitsplatz, der explosionsartigen Zunahme mobiler Geräte für die private und geschäftliche Nutzung und der Umstellung von Unternehmen auf vollständig dezentrale und hybride Arbeitsumgebungen ergeben haben, die Grenzen der VPN-Technologie für einen wirksamen Schutz von Geräten, Benutzer*innen und Daten in der modernen Bedrohungslandschaft aufgezeigt.

All diese Veränderungen haben die Art und Weise, wie wir mit Computern und mobilen Geräten arbeiten - und spielen - revolutioniert. Warum verlassen Sie sich also bei Ihrer Sicherheitsstrategie immer noch auf alte Prozesse, um die Sicherheit der in Bewegung befindlichen Daten zu gewährleisten?

Die kurze Antwort lautet Zero Trust Network Access, kurz ZTNA. Die lange Antwort ist, dass diese Lösung aus der realen Notwendigkeit heraus entwickelt wurde, verschiedene Gerätetypen, lokale und verteilte Benutzer*innen und Teams zu verwalten. Auch der Zugriff auf Daten über nicht vertrauenswürdige Netzwerke und das Vertrauen auf Cloud-basierte Dienste zur Erweiterung der Infrastruktur bei gleichzeitiger Aushöhlung der Netzwerkgrenzen des Unternehmens. Und das alles bei gleichzeitigem Schutz vor bestehenden und neuen Sicherheitsbedrohungen, die von Bedrohungsakteur*innen eingesetzt werden, wobei die Zahl der Bedrohungen, die auf macOS und mobile Geräte im Allgemeinen abzielen, deutlich zunimmt.

Einfach ausgedrückt: Die Sicherung von Netzwerkverbindungen ist nicht mehr nur für Mitarbeiter*innen auf Reisen oder für einige wenige Spezialfälle gedacht, um aus der Ferne produktiv zu bleiben.

Es geht auch über die bloße Verschlüsselung der Kommunikation zwischen zwei Punkten hinaus und erfordert granulare Sicherheitsvorkehrungen, um die Beteiligten zu schützen und den Zugriff auf Unternehmensressourcen zu verhindern, während die Einführung von Bedrohungen minimiert wird. ZTNA erreicht dies unter anderem durch folgende Maßnahmen:

- Integration mit Cloud-basierten IdPs, um zentral verwaltete Benutzerkonten, um Berechtigungen zu erweitern, die dem Benutzer/der Benutzerin folgen .
- Durch häufige Geräteüberprüfungen wird sichergestellt, dass die Endgeräte die Mindestanforderungen erfüllen, z. B. dass die Patches auf dem neuesten Stand sind, dass die Sicherheitsintegrität intakt ist, indem auf Jailbroken- oder Root-Geräte geprüft wird, und dass die Endpoint-Sicherheit ordnungsgemäß installiert und konfiguriert ist.
- Wenn Endpoints einen Gesundheitscheck nicht bestehen oder als gefährdet eingestuft werden, ermöglicht die ZTNA-Integration mit einer erstklassigen MDM-Lösung wie Jamf Pro eine richtlinienbasierte Verwaltung, indem Telemetriedaten sicher ausgetauscht werden, um den Zugriff zu sperren und Abhilfeworkflows auszuführen, um die notwendigen Aufgaben durchzuführen, um den Endpunkt in Übereinstimmung mit den Richtlinien zu bringen und zu überprüfen, ob alle erkannten Probleme behoben wurden.
- Verzicht auf implizites Vertrauen, wie bei herkömmlichen VPNs, und stattdessen Einsatz des Mantras „Niemals vertrauen - immer verifizieren” bei jedem Zugriff auf eine angeforderte Unternehmensressource. Erst nach erfolgreicher Überprüfung wird der Zugriff auf die angeforderte Ressource gewährt.

Was Sie für Daten im Transit benötigen

Eine sichere Netzwerkverbindung zu einem VPN-Server

So stellen Sie manuell eine Verbindung zu einem VPN her:

iOS und iPadOS

- Gehen Sie zu Systemeinstellungen > VPN
- Wählen Sie „VPN-Konfiguration hinzufügen”
- Geben Sie die Adresse des VPN-Servers auf dem Gerät ein
- Wählen Sie es aus Ihren Netzwerkoptionen aus
- Wiederholen Sie dies für jedes Gerät

macOS

- Gehen Sie zu Systemeinstellungen > Netzwerk > VPN & Filter
- Wählen Sie „VPN-Konfiguration hinzufügen”
- Geben Sie die Adresse des VPN-Servers auf dem Gerät ein
- Wählen Sie es aus Ihren Netzwerkoptionen aus
- Wiederholen Sie dies für jedes Gerät

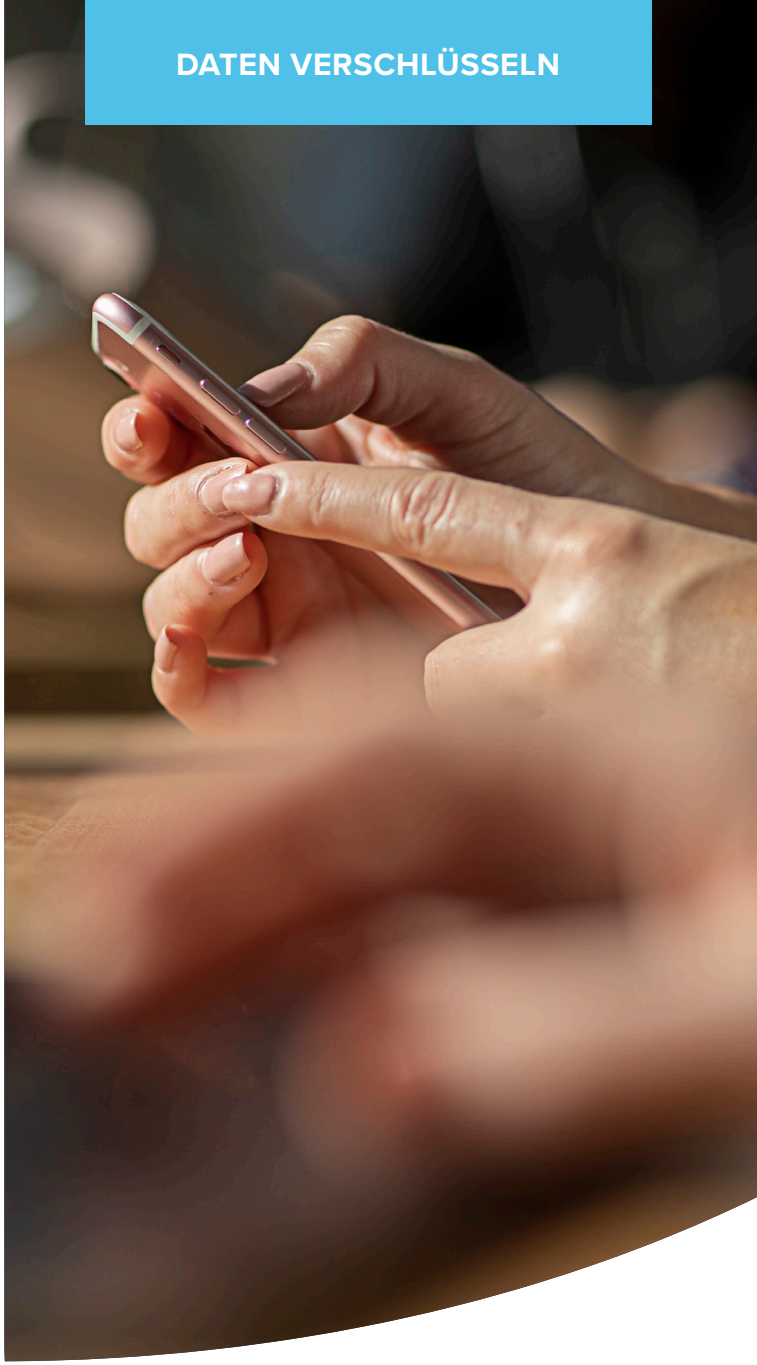
Um mehrere Geräte mit einem VPN zu verbinden:

Nachdem Sie einen VPN-Anbieter*innen eingerichtet haben

- Erstellen Sie ein Konfigurationsprofil in einem MDM wie Jamf für iOS und/oder macOS
- Bereitstellen von Konfigurationen auf beliebig vielen Geräten
- Sie haben es erraten — es gibt keinen Schritt drei

„Wie kann ich sicher sein, dass meine Verschlüsselung nahtlos ist?”

Eine wichtige Möglichkeit, Sicherheit und konsistente Verschlüsselung zu gewährleisten, besteht darin, Ihr MDM in der Cloud zu hosten. Mit einem seriösen Produkt wie Jamf Cloud können Sie sicher sein, dass Ihr Server und Ihre Daten geschützt sind und dass alle Updates oder Patches sofort verfügbar sind.



Vorteile von ZTNA gegenüber herkömmlichem VPN:

- Die Sicherheit wird durch den Wechsel von implizitem Vertrauen zum expliziten Zero-Trust-Modell verbessert, bei dem Benutzer und Geräte überprüft werden müssen, bevor Zugriff auf angeforderte Ressourcen gewährt wird.
- Split-Tunneling sichert den geschäftlichen Datenverkehr, während der private Datenverkehr direkt ins Internet geleitet wird - und nicht zurück in ein zentrales Netzwerk. Das reduziert den Overhead und spart Bandbreite, was zu einer höheren Leistung und einem besseren Schutz der Privatsphäre der Endbenutzer*innen führt.
- Always-on-Schutz bedeutet, dass Ressourcen auch dann geschützt sind, wenn der Dienst deaktiviert ist. Bei einer Zugriffsanfrage wird er automatisch aktiviert, um sicherzustellen, dass der Datenverkehr jedes Mal geschützt bleibt.
- Minimaler Platzbedarf und Cloud-Hosting bedeuten keine teuren Support-Verträge, komplexe Konfigurationen oder zu verwaltende Hardware.
- Es unterstützt auch macOS, iOS, iPadOS, Android und Windows, was die Gesamtbetriebskosten senkt und den Verwaltungsaufwand für IT-Teams, die mehrere Hardware- und Softwaretypen unterstützen, verringert.

In diesem Abschnitt haben wir die Grundlagen der Datenverschlüsselung besprochen, die Arten von Lösungen auf Apple Geräten erläutert und sogar die Schritte zur Aktivierung dieser Sicherheitskontrolle auf macOS, iOS und iPadOS erklärt. Wir haben auch erörtert, wie die moderne ZTNA-Technologie über den veralteten VPN-Schutz hinausgeht, indem sie weiterhin Remote Netzwerkverbindungen sichert und gleichzeitig zusätzliche Sicherheitsebenen enthält, um Benutzer*innen und Geräte zu verifizieren, bevor Zugriffsanfragen gewährt werden , und sicherzustellen, dass Daten im Ruhezustand (früher) und während der Übertragung (letzterer) sicher bleiben. Aber was ist, wenn Daten verwendet oder von Apps verarbeitet werden?

Entsperren Sie die beiden anderen Datenzustände; für Daten in Verwendung gibt es keine spezifische Sicherheitskontrolle zur Minderung dieses Risikos. Die Lösung liegt vielmehr in der Verbindung mit laufenden Verwaltungs- und Sicherheitsabläufen.

DATEN VERSCHLÜSSELN

Wenn Apps auf Daten zugreifen und diese verarbeiten, werden die Daten aus dem Arbeitsspeicher (RAM) zur Verarbeitung an die Anwendung weitergeleitet und dann zurück in den Arbeitsspeicher ausgelagert, bevor sie dauerhaft auf dem Speicher des Geräts gespeichert werden. Apps, die von bekannten, vertrauenswürdigen Entwickler*innen entwickelt werden, enthalten alle Sicherheitsmechanismen, die gewährleisten, dass die interne Sicherheit der App intakt bleibt. Einer der vielen Gründe dafür ist, dass sichergestellt werden muss, dass Daten, die innerhalb einer App verarbeitet werden, nicht mit anderen Apps, Diensten oder Prozessen, die auf dem Gerät laufen, geteilt werden oder durchgesickert sind. Damit soll die Integrität der Daten gewahrt werden, während die Integrität der App erhalten bleibt.

Apps, die durch die Ausnutzung einer Sicherheitslücke kompromittiert wurden, hatten unerlaubte Änderungen an ihrer internen Sicherheit oder sind „Rogue Apps", die als eine Aufgabe vermarktet werden und in Wirklichkeit andere, geheime Aufgaben ausführen.

Was ist also die beste Lösung, fragen Sie sich? Die folgenden Antworten umfassen eine Kombination aus bewährten Verfahren, einer Defense-in-Depth-Strategie sowie Prozessen und Workflows, die Jamf Pro nutzen, um die verwendeten Daten so sicher wie möglich zu halten:

- Eine kontinuierliche Patch-Management-Politik, die Apps aus legitimen Quellen bezieht, wie dem Apple App Store, der Website des Entwicklers oder von einem vertrauenswürdigen Verwaltungsanbieter - wie App Installers mit Jamf.
- Bereitstellung verwalteter Apps über Ihre bevorzugte MDM-Lösung und Implementierung einer richtlinienbasierten Verwaltung, um Anwendungen auf dem neuesten Stand zu halten.
- Überprüfung der sicheren Geräteeinstellungen durch die Installation von Konfigurationsprofilen, um die Möglichkeit von Bedrohungen durch Fehlkonfigurationen zu minimieren.
- Schränken Sie die Geräteeinstellungen ein, um riskante Verhaltensweisen einzuschränken, die zu Bedrohungen führen könnten, wie z. B. das Jailbreaking von iOS oder iPadOS oder das Side-Loading von Apps aus nicht autorisierten oder unsicheren Quellen.
- Implementierung eines fortlaufenden Schulungsprogramms für Benutzer*innen, um die Beteiligten über gängige Bedrohungen zu informieren und darüber, wie bestimmte Maßnahmen, wie z. B. Schatten-IT, Risiken mit sich bringen.
- Entwickeln Sie eine Acceptable Use Policy (AUP), die alle Beteiligten unterschreiben müssen, um sie auf die Verhaltenserwartungen und die Konsequenzen bei Verstößen gegen die Unternehmensrichtlinien hinzuweisen.

5

BAUSTEIN FÜNF:

Überwachung der Einhaltung der Compliance

Kenntnis des Status von Protokollen und Kontrollen, die auf allen Geräten vorhanden sind

Ein Sicherheitssystem ist nur so gut wie seine schwächste Stelle. Um eine optimale Abdeckung zu erreichen, müssen Administrator*innen die Geräte des Unternehmens überwachen, um sicherzustellen, dass jedes Gerät aktualisiert ist, die neuesten Patches erhalten hat und die richtigen Konfigurationsoptionen eingestellt sind.

„Das Bewusstsein der Unwissenheit ist der Anfang der Weisheit."

- Sokrates

Durch die kontinuierliche Erfassung umfangreicher Telemetriedaten, d. h. der Details jedes Geräts, die Aufschluss über die Sicherheitskontrollen, die Einstellungen und den Zustand des Geräts geben, kann die IT-Abteilung Geräte, Benutzer*innen und Daten besser schützen und gleichzeitig sicherstellen, dass Endgeräte, die nicht mehr in den Griff zu bekommen sind, schnell behoben und wieder konform gemacht werden, bevor Bedrohungen zu weitaus schlimmeren Folgen wie Datenschutzverletzungen führen können.

Wie bei den meisten Bausteinen in diesem E-Book gibt es auch bei der Überwachung der Endpoint-Compliance mehrere Wege: manuelle und automatische Methoden. Je nach den Anforderungen Ihres Unternehmens kann die Wirksamkeit der Compliance-Überwachung von verschiedenen Faktoren beeinflusst werden, z. B. von der Wissensbasis, den verwendeten Geräte- und Sicherheitsverwaltungslösungen und von budgetären Erwägungen, um nur einige der wichtigsten zu nennen.

Manuelles Überwachen und Verwalten des Bestands und der Einhaltung der Vorschriften bedeutet:

- Sicherstellen, dass alle Geräte in Ihrem Unternehmen geschützt sind, indem Sie die Geräte ständig überprüfen
- Physisches Aufspüren der einzelnen Geräte für die Bestandsverwaltung
- Individuelle Aktualisierung der Softwareapps auf jedem Gerät, um sicherzustellen, dass sie auf dem neuesten Stand sind
- Überprüfen Sie, ob die Sicherheitseinstellungen, z. B. die Verschlüsselung, auf allen Geräten einheitlich konfiguriert sind
- Überwachung und Bestätigung, dass niemand Risiken eingeführt hat, z. B. Malware oder verdächtige Apps
- Durchführung von Betriebssystem- und kritischen Sicherheitsupdates, sobald sie verfügbar sind, um bekannte Schwachstellen und Fehler in der Software zu beheben
- Einsatz von geeignetem Personal, um erkannte Probleme zu ordnen, gefährdete Geräte unter Quarantäne zu stellen und Abhilfemaßnahmen durchzuführen, um die betroffenen Endpoint-Geräte wieder konform zu machen

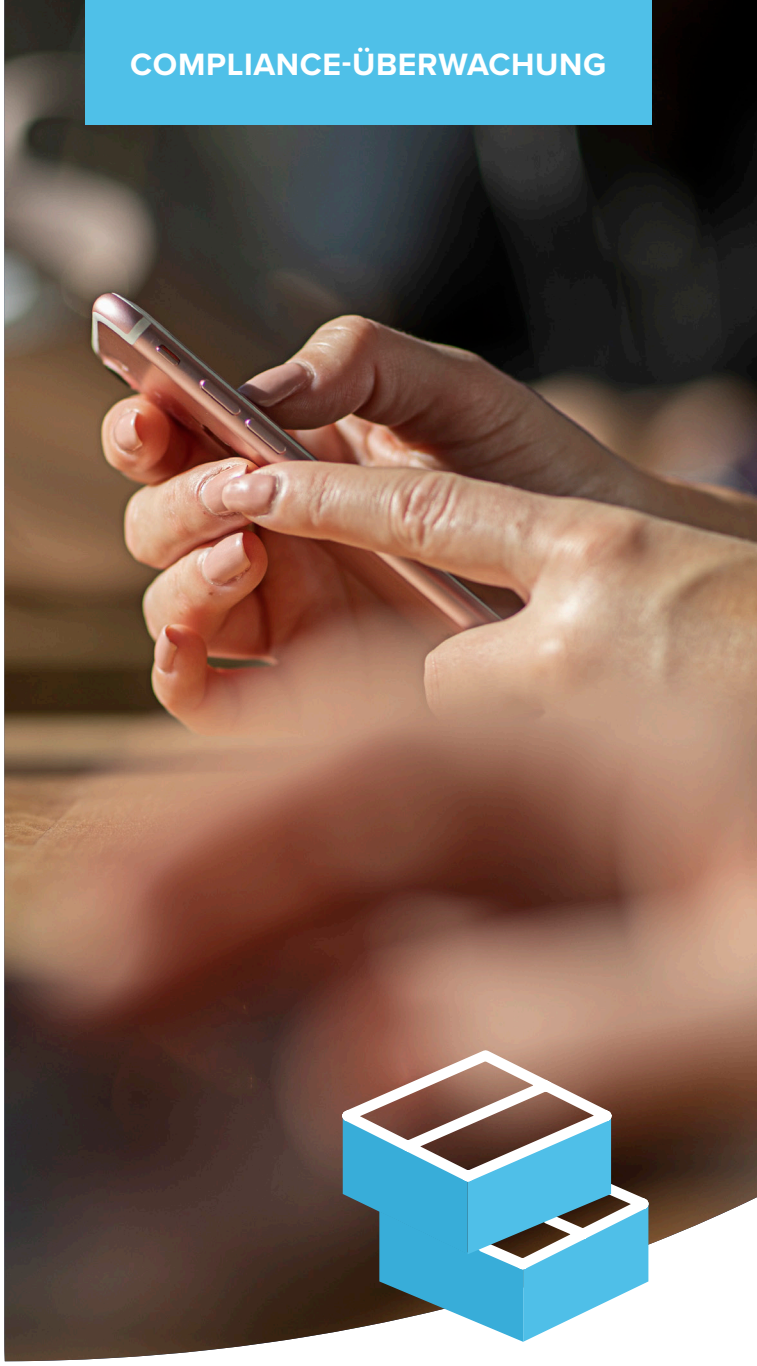
Diese Methode erfordert ständige Wachsamkeit und große Zeitfenster für den Verwaltungsaufwand, der mit der Erledigung von Verwaltungsaufgaben verbunden ist. Um erfolgreich zu sein, ist ein hohes Maß an Akzeptanz und Zusammenarbeit zwischen den Beteiligten und den Managementteams erforderlich. Es ist auch wichtig zu beachten, dass diese Methode weitgehend reaktiv ist, was bedeutet, dass zeitkritische Probleme, wie z. B. die Reaktionszeiten auf Vorfälle, wahrscheinlich verlängert werden, da sie erst nach der Entdeckung von Problemen auftreten - aber selten vorher.

Schließlich nimmt die Anzahl und Art der unterstützten Geräte zu, und die Zeit, die IT und Sicherheitskräfte benötigen, um manuell auf Probleme zu reagieren, steigt exponentiell an. Dadurch haben Bedrohungsakteure mehr Zeit, ihre Angriffskette gegen Unternehmen zu erweitern, was gleichzeitig das Risiko einer Datenverletzung erhöht.

Die Überwachung des Bestands mit Jamf bedeutet:

- Aktuelle Informationen in Echtzeit auf allen Geräten gleichzeitig anzeigen
- Bereitstellung von Updates und Sicherheitskonfigurationen für alle Geräte, die nicht ordnungsgemäß gesichert sind
- Sagen Sie es mit uns: **Es gibtkeinen dritten Schritt**

Die Möglichkeit, den Status des Gerätebestands einzusehen, hilft Administrator*innen, den Überblick über alle Apple Geräte in ihrer Flotte zu behalten. Wenn Administrator*innen den aktuellen Status eines Geräts kennen, können sie Geräte und Sicherheit effizient verwalten, indem sie wissen, welche Updates wohin zu senden sind und welche Sicherheitsfunktionen entsprechend zu konfigurieren sind. Die Erstellung intelligenter Gruppen auf der Grundlage dynamischer Kriterien bedeutet, dass Administrator*innen bei Aktualisierungen so gezielt oder umfassend vorgehen können, wie sie möchten. Ob auf der Grundlage von granularen Berechtigungen, bestimmten Gerätetypen oder praktisch jeder anderen Kategorisierungsmethode, Jamf Pro bietet leistungsstarke Tools, um die Arbeit mit Compliance-bezogenen Aufgaben zu erleichtern und gleichzeitig die Flexibilität zu bewahren, Aufgaben anhand von anpassbaren Kriterien auf Null zu setzen (oder an alle Geräte in Ihrer Flotte zu senden). Erfahren Sie mehr in unserem E-Book Bestandsmanagement für Einsteiger*innen.



Die Einhaltung der Jamf Vorschriften zu verwalten bedeutet:

- Prüfung von Endpoints auf der Grundlage von Benchmarks des Center for Internet Security (CIS)
- Streamen Sie alle Ihre Compliance-Daten in die Cloud für eine zentrale Verwaltung
- Zugriff auf einheitliche macOS Protokolle und umfassende Endpoint-Telemetrie, um Bedrohungen schnell und effizient zu identifizieren
- Durchsetzung der Konformität mithilfe von Richtlinien zur Automatisierung von Abhilfemaßnahmen und zur Überwachung von Endpoints
- Überwachen Sie nach Common Vulnerabilities and Exposures (CVE), um die in Ihrer Umgebung vorhandenen Schwachstellen zu erkennen
- Vorbeugung von Sicherheitsbedrohungen mithilfe umfassender Analysen, die dem MITRE &TTACK-Framework entsprechen
- Sicherer Austausch von Telemetriedaten zwischen Management- (Jamf Pro) und Sicherheitslösungen (Jamf Protect) über API, um fortschrittliche Arbeitsabläufe zu entwickeln, mit denen die Reaktionszeiten auf Vorfälle automatisch minimiert und erkannte Probleme ohne Verzögerung gelöst werden können

IEs reicht nicht aus, Ihre Geräte zu sichern; viele Vorschriften verlangen, dass Unternehmen nachweisen können, dass die Geräte weiterhin sicher sind und die Compliance-Anforderungen erfüllen. Das bedeutet, dass Unternehmen Unterlagen vorlegen müssen, um die Einhaltung der Vorschriften zu verschiedenen Zeitpunkten zu belegen. Denn wenn Sie nicht nachweisen können, dass das Gerät zu einem bestimmten Zeitpunkt konform war, dann war es in jeder Hinsicht nicht konform.

Die Daten und Berichte von Jamf geben Unternehmen jedoch die notwendigen Tools an die Hand, um Telemetriedaten von jedem Endpunkt zu erhalten und diese Daten anhand wichtiger Kategorisierungen wie Patch-Levels, entdeckte Schwachstellen und Zeitstempel, die während des Lebenszyklus des Geräts durchgeführte Aktionen identifizieren, zu organisieren. Darüber hinaus ermöglicht die Integration den sicheren Austausch von Telemetriedaten mit Tools von Erst- und Drittanbieter*innen, um die Daten durch zentralisierte Dashboards mit Datenvisualisierungen und den Export in andere Formate für die Weitergabe von Compliance-Berichten an Prüfer*innen zu erweitern.

6

BAUSTEIN SECHS:

Appsicherheit und -management

Patch-Berichte, Richtlinien und App-Installer, um Apps auf dem neuesten Stand zu halten und gleichzeitig die Sicherheit zu gewährleisten.

Appsicherheit

Die Gewissheit, dass erkannte Schwachstellen gepatcht werden, ist für die Sicherheit des Geräts von entscheidender Bedeutung. Aber wissen Sie auch, woher Ihre Bewerbungen kommen? Und sind Sie sicher, dass sie keine Malware oder anderen bösartigen Code enthalten? Die Antwort auf diese Fragen ist für Ihr Unternehmen von entscheidender Bedeutung, denn wenn Sie Ihren Appquellen nicht vertrauen können, riskieren Sie die Sicherheit Ihrer Geräte, die Privatsphäre der Endbenutzer*innen und die Preisgabe sensibler Daten.

Für Apple hat die Wahrung von Sicherheit und Privatsphäre höchste Priorität. Wenn es um die Sicherheit von Apps geht, machen sie das Herunterladen und die Nutzung von Apps so sicher wie möglich.

Merkmale der Appsicherheit und -verwaltung:

1 **Apps laufen in einer Sandbox:** Jede App läuft in ihrem eigenen Bereich und kann nicht mit anderen Apps interagieren. Bevor Apps die gemeinsam genutzten Daten anderer lesen/schreiben können, ist die ausdrückliche Genehmigung eines authentifizierten Benutzers/einer authentifizierten Benutzerin erforderlich.

2 **Zentralisierte und sichere App-Beschaffung:** Apps im App Store von Apple werden überprüft, um Sicherheitsrisiken zu verringern. Ein Teil davon wird durch notarielle Beglaubigung erreicht, während der andere Teil ein sicheres, von Apple verwaltetes Cloud-basiertes Repository bereitstellt, in dem Apps gehostet werden, die strenge Sicherheitsprüfungen bestanden haben. Außerdem können die Entwickler*innen die neueste Version ihrer gehosteten Apps direkt in die Hände der Nutzer*innen geben, sodass die Gefahr des Herunterladens illegaler Software aus riskanten Quellen ausgeschlossen ist.

3 **Die notarielle Beglaubigung bestätigt die Sicherheitsintegrität:** Die notarielle Beglaubigung von Apps gibt den Nutzer*innen mehr Sicherheit, dass Software, die mit der eindeutigen ID eines Entwicklers/einer Entwicklerin signiert und auf den Mac geladen wurde, von Apple auf bösartige Komponenten und Code-Signierungsprobleme geprüft wurde. Wenn eine App notariell beglaubigt ist, können Sie darauf vertrauen, dass sie nicht manipuliert oder kompromittiert wurde.

4 **Gatekeeper blockiert die Ausführung verdächtiger Apps:** Bevor eine macOS App zum ersten Mal ausgeführt werden darf (und nach jeder nachfolgenden Aktualisierung), werden zugewiesene Beglaubigungstickets mit Gatekeeper abgeglichen, um festzustellen, ob das Ticket gültig oder widerrufen ist. Im ersten Fall kann die App ohne Probleme ausgeführt werden. Ist Letzteres der Fall, wird die Ausführung der App eingeschränkt und der Benutzer/die Benutzerin darüber informiert, dass sie möglicherweise von einem Unbefugten geändert wurde, was die Integrität der internen Sicherheit beeinträchtigt.

5 **Beschränkungen für die App-Nutzung:** Auf iOS basierten Geräten ist der einzige sichere Weg, Apps zu erhalten, der App Store. Allerdings bietet das Jailbreaking von iOS und iPadOS Geräten die Möglichkeit, auf App-Stores von Drittanbieter*innen zuzugreifen, über die häufig Apps vertrieben werden, die „geknackt" wurden oder deren interne Sicherheitsvorkehrungen entfernt wurden, wie z. B. kostenpflichtige Apps, die zwar kostenlos zur Verfügung gestellt werden, aber häufig von Bedrohungsakteuren mit bösartigem Code versehen wurden, um Daten zu stehlen oder Nutzer*innen auszuspionieren. Mit einem MDM wie Jamf Pro können Administrator*innen Warnmeldungen einrichten, die sie benachrichtigen, wenn Jailbroken-Geräte identifiziert werden, so dass sie Workflows zur Behebung des Sicherheitsproblems durchführen können.

Unter macOS können Benutzer*innen (oder Administrator*innen mit einem MDM) zwischen zwei Gatekeeper-Optionen wählen:

- Mac App Store
- Mac App Store und identifizierte Entwickler*innen

Die Beschränkung von macOS Nutzer*innen auf den Mac App Store für ihre Apps ermöglicht es Administrator*innen, die App-Sicherheit geräteübergreifend zu kontrollieren und gleichzeitig das Risiko der Einschleppung von Bedrohungen - ob bösartig oder nicht - durch verdächtige, riskante und/oder gefährdete Apps zu minimieren. Wenn Sie jedoch Apps von Drittanbieter*innen benötigen, die nur auf der Website des Entwicklers/der Entwicklerin verfügbar sind, ermöglicht die zweite Option den Bezug von Apps sowohl aus dem App Store als auch von identifizierten Entwickler*innen, die von Apple überprüft wurden und Softwarepakete erstellen, die mit ihrer jeweiligen Entwickler*innen-ID signiert sind, um die Sicherheit zu erhöhen.

Best Practices

Für macOS sollten Sie den Mac App Store und die Auswahl der identifizierten Entwickler*innen konfigurieren, insbesondere wenn Sie Ihre eigenen Apps erstellen oder Apps für die Bereitstellung neu verpacken. Beantragen Sie außerdem eine Entwickler*innen-ID bei Apple und signieren Sie intern von der Organisation entwickelte Apps, damit Gatekeeper ihnen vertraut. Durch die Verwendung von Jamf Pro als MDM Lösung kann der Self-Service-App-Katalog auf allen Geräten bereitgestellt werden, wobei die IT-Abteilung den Endbenutzer*innen Apps, Einstellungen, Konfigurationen und vieles mehr vorab genehmigt, sodass sie auf die benötigten Tools und Dienste zugreifen und diese installieren können, wenn sie sie benötigen, ohne dass ein Helpdesk-Ticket, eine Änderung der Berechtigungen oder eine Apple ID erforderlich sind.

Manuelle Einrichtung der Gatekeeper-Optionen:

- Navigieren Sie zu: Systemeinstellungen > Datenschutz und Sicherheit > Sicherheit
- Wählen Sie eine der beiden verfügbaren Optionen
- Wiederholen Sie diesen Vorgang für jedes Gerät in Ihrem Unternehmen

Einrichten von Gatekeeper-Optionen mit Jamf Pro:

- Richten Sie ein Konfigurationsprofil mit Ihren Gatekeeper-Einstellungen ein und verteilen Sie es auf alle Ihre Geräte.
- **Das war´s!**

App- und Sicherheits-Patches und -Updates

Betriebssystem-Updates, Versionskontrolle mit MDM-Befehlen, schnelle Sicherheitsreaktionen und mehr

Unternehmen müssen eine Patch-Management-Strategie implementieren, um Fehlerbehebungen so schnell wie möglich zu testen und einzupflegen, damit ihre Hardware, Daten und Benutzer*innen geschützt sind. Testen ist eine oft übersehene Notwendigkeit bei der Bereitstellung von Patches, insbesondere wenn Fehler in Form von Sicherheitslücken auftreten, die so schnell wie möglich behoben werden müssen. Indem die IT-Abteilung beides so schnell wie möglich durchführt, reduziert sie die Auswirkungen von Sicherheitsbedrohungen, die sich ausbreiten, und minimiert gleichzeitig größere Probleme, die sich aus Patches ergeben, die eine Sache beheben, aber unbeabsichtigt andere, kritischere Funktionen beeinträchtigen.

In diesem E-Book ist der Trend, wie lange die Erledigung von Verwaltungsaufgaben durch die IT-Abteilung dauert, direkt mit der Anzahl der verwalteten Geräte korreliert. Bei der Verwaltung von Patches gilt diese Regel nach wie vor, mit einer Ausnahme: Die Anzahl der erforderlichen Patches kann von wenigen bis zu vielen reichen, was den Verwaltungsaufwand pro Gerät um eine unbekannte Anzahl erhöht.

Sehen wir uns einige der Optionen an, die Administrator*innen bei der manuellen und der MDM Verwaltung von Patches zur Verfügung stehen:

Optionen für die manuelle Verwaltung von Patches:

- Bringen Sie den Nutzer*innen bei, Aktualisierungen selbst durchzuführen, sobald sie Aktualisierungsbenachrichtigungen auf ihren Geräten erhalten.
- Sammeln Sie alle Geräte, wenn ein neuer Patch veröffentlicht wird, und verteilen Sie ihn manuell.
- Reparieren Sie Geräte mit fehlenden Patches im Rahmen Ihrer laufenden Compliance-Überwachung.

Optionen für die Verwaltung von Patches über MDM (d.h. Jamf Pro):

- Updates und Patch-Benachrichtigungen werden automatisch von Jamf empfangen, zusammen mit Tools für die Bereitstellung von Patches auf allen Geräten Ihres Unternehmens, sodass Sie nach Ihrem Zeitplan aktualisieren können - und nicht nach dem eines anderen.
- Der Self-Service-App-Katalog von Jamf macht es den Benutzer*innen leicht, ein Update durchzuführen, sobald ein neuer Patch verfügbar ist, indem er die Benutzer*innen benachrichtigt, dass sie ein Update durchführen müssen, bevor sie eine betroffene App weiter nutzen können.
- Eliminieren Sie die Abhängigkeit von Endbenutzer*innen und entlasten Sie die IT-Abteilung durch die Automatisierung der Patch-Verteilung. Versenden Sie Patches als Richtlinien an alle Geräte, oder zielen Sie mit dynamischen Smart Groups darauf ab, um sicherzustellen, dass die Geräte auf dem neuesten Stand sind.

Wenn Sie mehr über den Lebenszyklus von Apps und die Automatisierung und Bereitstellung von Apps erfahren möchten, lesen Sie unser Whitepaper.

Erhöhen Sie Ihre Sicherheit

Falls Sie es noch nicht gemerkt haben: Sicherheit ist keine Einheitslösung. Eine umfassende Strategie, die Ihre Geräte, Benutzer und Daten ganzheitlich schützt und gleichzeitig granulare Schutzmaßnahmen bietet, die sich zu einem digitalen Sicherheitsnetz zusammenfügen, besteht aus mehreren Ebenen. Dies wird als Tiefenverteidigung bezeichnet, d. h., wenn eine Schicht eine Bedrohung nicht abfängt, ist die nächsthöhere oder -tiefere Schicht da, um sie einzudämmen.

Wahrscheinlich sind Sie bereits mit dem mehrschichtigen Sicherheitsansatz vertraut und wissen es vielleicht nicht einmal. Nehmen wir als Beispiel etwas, mit dem Sie sehr vertraut sind: Ihr Zuhause.

Mit der Mischung aus alten und neuen Sicherheitsvorkehrungen, die für die Sicherheit zu Hause zur Verfügung stehen, haben Sie zweifellos einige (oder vielleicht sogar alle) Vorkehrungen getroffen, um Ihre Lieben und sich selbst zu Hause zu schützen:

- Riegelschlösser an Ihren Türen
- Hausalarmanlage
- Überwachung durch Videokameras
- Sicherheitspersonal, das auf dem Gelände patrouilliert
- Rauch- und Kohlenmonoxiddetektoren
- Feuerlöscher
- Versicherung für Hausbesitzer oder Mieter*innen

Jede der oben genannten Lösungen kann theoretisch auch als Einzellösung für die Sicherheit des Hauses eingesetzt werden. Aber für sich genommen bietet sie nur einen Teil der erforderlichen Gesamtsicherheit, oder? Kombiniert man sie jedoch, fügen sich die verschiedenen Teile wie ein Puzzle zusammen, um das Gesamtbild zu veranschaulichen und das gesamte Spektrum der Probleme umfassend zu erfassen. Cybersicherheit und die Verwaltung und Sicherheit Ihrer Apple Geräteflotte beruhen auf ähnlichen Grundsätzen und bilden den Kern der Befähigung und Information der Nutzer*innen, gute Sicherheitspraktiken zu haben und zu befolgen, um Risiken zu minimieren und Bedrohungen abzuschwächen.

Eine solche Ebene der Endpoint-Sicherheit ist die Warnung vor Risiken für Geräte. Einige Benutzer*innen können beispielsweise einen Phishing-Angriff erkennen und deshalb noch nicht auf einen bösartigen Link klicken; andere Benutzer*innen sind vielleicht etwas zu vertrauensselig und führen die Anweisungen des bösartigen Links aus, wodurch sie möglicherweise ein Risiko für das Gerät, den Benutzer*innen und die Daten darstellen. Wie würde der betroffene Benutzer*innen überhaupt wissen, dass er auf einen bösartigen Link geklickt oder eine Aktion durchgeführt hat, die sein Gerät oder seine Anmeldeinformationen gefährdet hat?

Dafür gibt es eine App! Jamf Trust schützt vor Benutzer*innen initiierten Risiken, wie dem obigen Beispiel eines Phishing-Angriffs, indem es die Benutzer in Form von Apple Push-Benachrichtigungen benachrichtigt, wenn Jamf eine Bedrohung auf ihrem Gerät erkennt - etwa wenn der bösartige Link, auf den geklickt wurde, zuvor bösartigen Code in Form von Malware geliefert hat, die gerade die Tastenanschläge auf dem Gerät aufzeichnet.

Die Lösung hat das Vorhandensein einer Bedrohung festgestellt und den Benutzer/die Benutzerin (und auch den Administrator*innen) informiert. Die IT-Abteilung kann auf den Vorfall reagieren und ihn schnell beheben, indem sie eine Kombination aus Jamf Pro und Jamf Protect einsetzt, um das Gerät vom Netzwerk zu isolieren, die Infektion zu beseitigen, alle vorhandenen Schwachstellen zu patchen und den Ausgangszustand des Geräts wiederherzustellen. Und schließlich sollten die gewonnenen Erkenntnisse in künftige Sicherheitsschulungen für die Beteiligten einfließen.

Geräte- und Datensicherheit ist nicht zum Lachen.

Unternehmen haben die Möglichkeit, vielen möglichen Angriffen oder Datendiebstählen einen Schritt voraus zu sein, indem sie die bestmöglichen Sicherheitsvorkehrungen durch Apple implementieren — und Jamf kann dies einfacher, schneller und weitaus sicherer und effizienter machen als manuelle Sicherheitsprotokolle.

Wenn es um Cybersicherheit geht, mag niemand Überraschungen und möchte auf keinen Fall auf einen Angriff reagieren müssen, wenn er es vermeiden kann. Holen Sie sich die besten Sicherheitsoptionen für Ihr Unternehmen, indem Sie die Produktlösungen von Jamf kostenlos testen. Oder nehmen Sie noch heute Kontakt mit einem Jamf Vertreter*innen auf, um zu besprechen, wie eine maßgeschneiderte, umfassende Apple Verwaltungs- und Sicherheitslösung für die individuellen Anforderungen Ihres Unternehmens aussehen kann.

Sie haben den Rest ausprobiert... jetzt nehmen Sie das Beste!

Versuchen Sie Jamf

Oder wenden Sie sich an Ihren bevorzugten Reseller für Apple Geräte, um eine kostenlose Testversion zu erhalten.