jamf

Verständnis von Sicherheits-frameworks

Cybersicherheitspläne zur Risikominimierung und zum Schutz des Unternehmens vor Bedrohungen minimieren potenzielle Angriffsvektoren. Die Auswirkungen einer ganzheitlichen Sicherheitsstrategie sind von Unternehmen zu Unternehmen völlig unterschiedlich, da sie die individuellen Bedürfnisse der einzelnen Unternehmen berücksichtigt. Unmittelbar mit den Bedürfnissen verknüpft ist die Rolle, die die Einhaltung von Vorschriften spielt. Und das, bevor man sich die unzähligen Möglichkeiten vorstellt, die die Sicherheit von Unternehmen durch bösartige Akteur*nnen in der modernen Bedrohungslandschaft beeinträchtigen.

Angesichts all dieser Variablen könnte man meinen, dass die Erstellung eines Cybersicherheitsplans viel schwieriger ist, als es scheint, aber das muss nicht sein.

Sicherheitsframeworks und die Vorteile, die sie für Unternehmen aller Größen und Branchen bieten, ganz zu schweigen von ihrer Rolle bei der Entwicklung kohärenter Strategien zur Minimierung von Risikofaktoren, der Einhaltung von Compliance-Zielen und vielem mehr.

Was den Lebenszyklus der Cybersicherheit betrifft, so spiegeln die umfassende Implementierung und die laufende Verwaltung von Cybersicherheitskontrollen und -lösungen direkt die erfolgreiche Verwaltung von Informationssicherheitsrisiken in Ihrem Unternehmen wider - oder auch das Scheitern dieser Bemühungen.

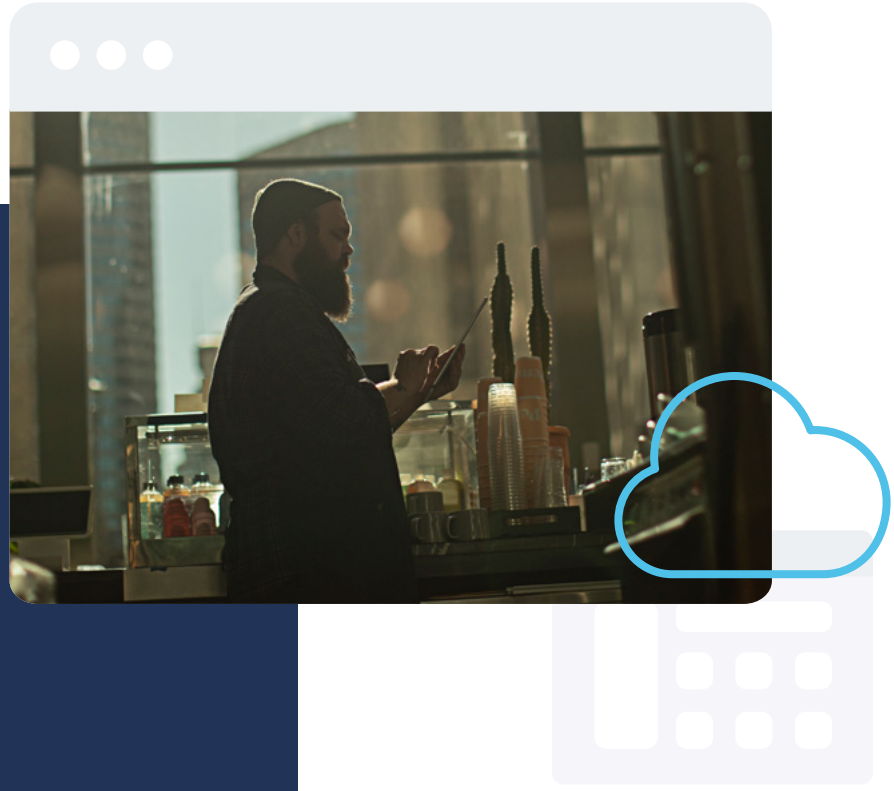
Der Erfolg eines Cybersicherheitsplans hängt von folgenden Faktoren ab

- Die Größe Ihrer Organisation
- Haushaltszwänge
- Regulatorische Anforderungen (falls zutreffend)
- Einzigartige Anforderungenan die Kontinuität des Geschäftsbetriebs
- Umfassende und genaue Risikobewertungen
- Wissensbasisund Fähigkeiten der IT- und Sicherheitsteams

Die obige Liste ist zwar nicht erschöpfend, zeigt aber die wichtigsten Punkte auf, die für den Erfolg eines jeden Sicherheitsplans entscheidend sind. Selbst wenn Unternehmen mit diesen Informationen ausgestattet sind, kann es für sie entmutigend sein, mit der Arbeit zu beginnen, einfach weil es **andere Variablen gibt, die sie nicht** kennen, oder weil Einschränkungen bei einem der oben genannten Faktoren zu Herausforderungen führen können, wenn sie versuchen, die richtige Kombination aus Hardware, Software, Konfigurationen, Richtlinien und Arbeitsabläufen zu finden, um die einzigartigen Cybersicherheitsanforderungen Ihres Unternehmens zu erfüllen.

Frameworks beheben diese und viele andere Fallstricke, die in Informationssicherheitsstrategien vorhanden sein können, indem sie Unternehmen einen klaren, präzisen Fahrplan bieten, den sie bei der Ausarbeitung oder Verwaltung ihrer bestehenden Cybersicherheitspläne befolgen können.

WAS SIND FRAMEWORKS?



Wir haben das Wort „Fahrplan“ verwendet, um die oben genannten Rahmen zu beschreiben. Ein anderer, technisch vielleicht genauerer Ausdruck wäre „Blaupause“. Ähnlich wie ein Bauunternehmer/eine Bauunternehmerin einen Bauplan verwendet, um ein strukturell solides Gebäude zu errichten, können (und sollten) IT- und Sicherheitsteams eine der vielen verschiedenen Arten von Frameworks verwenden, um einen Sicherheitsplan zu entwickeln, der darauf abzielt:

- Identifizieren
- Schutz
- Erkennung
- Antworten
- Wiederherstellen

Die implementierten Frameworks sollten zusammenarbeiten, um das Cybersicherheitsrisiko durch prägnante, organisierte und in der Branche anerkannte bewährte Verfahren und Methoden zu mindern.

ARTEN VON FRAMEWORKS

Es gibt mehrere verschiedene Frameworks. Sie befassen sich jeweils mit einer bestimmten Komponente der Informationstechnologie oder der Informationssicherheit und stärken diese. Einige bieten allgemeine Anleitungen für den Schutz Ihrer Infrastruktur vor aktuellen und sich entwickelnden Bedrohungen, andere informieren über die Verbesserung von Prozessen, die die Effizienz von IT-Verwaltungsdiensten steigern. Andere hingegen konzentrieren sich ausschließlich auf die Stärkung Ihrer Sicherheitslage in bestimmten Sicherheitsszenarien, z. B. in regulierten Umgebungen, wie dem Gesundheits-, Finanz- oder Bildungswesen.

GEMEINSAME FRAMEWORKS UND VORSCHRIFTEN FÜR DIE CYBERSICHERHEIT

FRAMEWORKS

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v1.1: Das NIST untersteht dem US-Handelsministerium und hat den Auftrag, die Wettbewerbsfähigkeit der Industrie zu fördern. Diese Programme erstrecken sich auf verschiedene Labore, darunter auch Informationstechnologie und Sicherheit. Das CSF stellt eine fortlaufende gemeinsame Anstrengung von Industrie, Wissenschaft und Regierung dar, um kritische Cybersicherheitsinfrastrukturen zu verbessern, deren Ausnutzung finanzielle und Reputationsrisiken verursacht.

NIST Special Publication (SP) 800-53, Rev. 5: Befasst sich mit Sicherheits- und Datenschutzrisiken, indem es einen Katalog von Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen vor einer Vielzahl von Bedrohungen und Risiken bereitstellt, einschließlich, aber nicht beschränkt auf Fehlkonfiguration, bösartige Akteur*innen und menschliches Versagen. Die enthaltenen Kontrollen sind flexibel und anpassbar und helfen Unternehmen, Risiken zu minimieren und gleichzeitig die Funktionalität und Sicherheit von Computersystemen zu gewährleisten.

ISO/IEC 27001: Diese Norm definiert die Anforderungen, die Informationssicherheits-Verwaltungssysteme (ISMS) erfüllen müssen, und bietet gleichzeitig eine Anleitung für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Verwaltungssystems. Er berücksichtigt bewährte Praktiken und Grundsätze innerhalb eines international anerkannten Standards, der für Unternehmen aller Größen und Branchen gilt.

MITRE ATT&CK: Hierbei handelt es sich um eine globale Wissensbasis über die von Cyber-Angreifer*innen verwendeten Taktiken, die auf Beobachtungen realer Techniken beruht. Sie bildet die Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und Methoden für verschiedene Branchen, Gemeinschaften und Endpunktsicherheitslösungen.

FRAMEWORKS

American Institute of Certified Public Accounts (AICPA) System- und Organisationskontrollen (SOC): Eine Reihe von Berichten, die drei Arten von Berichten umfassen: SOC 1, SOC 2 und SOC 3. Sie bieten detaillierte Informationen und Gewissheit über die Kontrollen in einer Dienstleistungsorganisation, die für die Sicherheit, Verfügbarkeit und Verarbeitungsintegrität der Systeme, die für die Handhabung und Verarbeitung sensibler Daten verwendet werden, relevant sind, und bieten gleichzeitig eine validierte Gewissheit über die Kontrollen durch die Nutzer*innen dieser Dienstleistungen.

Zentrum für Internet-Sicherheit (CIS): Die CIS-Benchmarks sind präskriptive Konfigurationsempfehlungen für mehr als 25 Produktfamilien von Anbieter*innen. Jeder Benchmark bietet sichere Konfigurationsleitfäden, die als Teil einer konsensbasierten Bemühung globaler Cybersicherheitsexpert*innen entwickelt wurden und von Regierungen und Industrien weltweit akzeptiert und verwendet werden und die Grundlage für einige Endpointtsicherheitslösungen bilden.

macOS Security Compliance Project (mSCP): Dieses Projekt ist ein Open-Source-Projekt, bei dem die Mitarbeiter*innen des NIST, der National Aeronautics and Space Administration (NASA), der Defense Information Systems Agency (DISA) und des Los Alamos National Laboratory (LANL) zusammenarbeiten, um einen programmatischen Ansatz für die Erstellung von Sicherheitsrichtlinien zu entwickeln, einschließlich Konfigurationseinstellungen, mit denen die Einhaltung bestimmter gesetzlicher Vorgaben speziell für die Sicherung und Einhaltung von Apple macOS erreicht werden soll.

VORSCHRIFTEN

Healthcare Insurance Portability and Accountability Act (HIPAA): Modernisiert den Informationsfluss im Gesundheitswesen und enthält Anforderungen für den Umgang mit geschützten Gesundheitsinformationen (PHI), einschließlich der Festlegung von Beschränkungen für die Weitergabe von Gesundheitsdaten von Patient*innen und der Konsequenzen bei Verstößen gegen das Gesetz.

Sarbanes-Oxley-Gesetz von 2002 (SOX): Dieses Bundesgesetz schreibt verbindliche Praktiken für die Aufzeichnung und Berichterstattung von Finanzangelegenheiten für Organisationen im Finanzsektor vor.

Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS): Ein EU-Mandat der Agentur der Europäischen Union für Cybersicherheit (ENISA) verlangt von den Mitgliedsstaaten, dass sie Vorschriften in ihre jeweiligen nationalen Gesetze aufnehmen, um das Niveau des Cybersicherheitsschutzes zu erhöhen, das von der Meldung von Sicherheitsvorfällen bis hin zur Behandlung durch Reaktionsteams reicht.

Allgemeine Datenschutzverordnung (GDPR): Dieses auf den Datenschutz ausgerichtete Sicherheitsgesetz wurde für Europa entwickelt, wirkt sich jedoch auf alle Organisationen aus, die Daten von EU-Bürger*innen verarbeiten. Die Richtlinien zur Einhaltung der Vorschriften decken alle Aspekte des Datenschutzes ab, darunter Verfahren für den Umgang mit Cookies, ePrivacy und das „Recht auf Vergessenwerden“ der Nutzer*innen.

Family Educational Rights and Privacy Act (FERPA): Dieses US-Bundesgesetz schützt die Privatsphäre der Schüler*innen und die Daten in den Bildungsunterlagen, einschließlich des Zugriffs auf diese Informationen und des Rechts, falsche Informationen zu ändern. Bei Minderjährigen wird dieses Recht auf die Eltern oder den Vormund ausgedehnt; wenn der Student/die Studentin jedoch die Volljährigkeit erreicht (18 in den USA) oder eine Hochschule besucht, gehen diese Rechte allein auf ihn über.

VERWENDUNG VON FRAME-WORKS ALS TEIL EINER UMFAS-SENDEN SICHER-HEITSSTRATEGIE

Die Implementierung von Frameworks zur Stärkung Ihrer Sicherheitslage durch die Berücksichtigung von Schlüsselfaktoren auf der Grundlage bewährter Verfahren und solider Methoden muss keine schwere Aufgabe sein. Das kann sein, aber wenn es richtig gemacht wird, kann es Teil Ihres Sicherheitsplans sein und sich nahtlos in Ihre Sicherheitstools integrieren, um die Einhaltung von Vorschriften durch sichere Prozesse und Arbeitsabläufe durchzusetzen.

Es gibt die „altmodische“ Methode, Frameworks in Ihre bestehende Verwaltungsstrategie einzubinden, bei der Sie eine aktuelle Bewertung Ihrer Sicherheitslage manuell mit einer Liste der oben genannten Frameworks vergleichen und die Liste Punkt für Punkt durchgehen, um zu ermitteln, welche Konfigurationen, Einstellungen, Protokolle, Prozesse, Arbeitsabläufe und Richtlinien nicht den Anforderungen entsprechen. Und das ist nur der erste Teil des manuellen Prozesses. Der zweite Teil umfasst die manuelle Korrektur aller Komponenten, die nicht in den Geltungsbereich fallen, um sie in Übereinstimmung mit den Vorschriften zu bringen.

Da sich die Sicherheit ständig ändert, ist dies auch kein einmaliger Prozess. Sie muss in regelmäßigen Abständen durchgeführt werden, um zu überprüfen, ob die Endpoints gesichert sind und ob sie die Vorschriften einhalten.

Die folgenden Herausforderungen wirken sich erheblich auf die Häufigkeit, die Genauigkeit und den Erfolg der manuellen Anpassung von Frameworks in Ihrem Cybersicherheitsplan aus:

- Anzahl und Typen der Geräte in Ihrer Flotte
- Größe und Fähigkeiten Ihrer IT- und Sicherheitsteams
- Ressource nwie Zeit und Geld, die für die Durchführung dieses Prozesses bereitgestellt werden
- Grad der Unterstützung durch die Führung
- Konkurrierende Anforderungen an die Geschäftskontinuität
- Auswirkungen auf die Benutzerproduktivität, Ausfallzeiten und Blockierer
- Bestehende Sicherheitstools und ihre Fähigkeiten

Nachdem wir den manuellen Prozess aus dem Weg geräumt haben, wollen wir uns nun dem zuwenden, was Administrator*innen wirklich wollen - eine automatisierte Methode zur Implementierung von Frameworks in ihren Cybersicherheitsplan. Eine, die den bereits überlasteten IT- und Sicherheitsteams keine zusätzliche Arbeit aufbürdet, sondern stattdessen hilft:

- Sicherheitsbedenken schnell und effizient ausräumen
- Nahtlose Integration mit den besten Verwaltungstools
- Hinzufügen von erweiterten Workflows und richtlinienbasierter Verwaltung zur Automatisierung von Abhilfemaßnahmen
- Teams jeder Größe durch den Einsatz von Sicherheitstools, die schwere Aufgaben übernehmen
- Entlastung des Verwaltungsaufwands, sodass die Zeit besser für andere Aufgaben genutzt werden kann
- Ständige Überwachung der Endpoints, die einen Echtzeit-Einblick in den Gerätezustand bietet
- Cloud-basierte Lösungen ermöglichen die Entschärfung von Geräten von jedem Ort und zu jeder Zeit
- Automatisierung des laufenden Prozesses durch dynamische Anpassung an Änderungen der Sicherheitslage, um die Einhaltung von Frameworks und sich entwickelnden Sicherheitsanforderungen durchzusetzen

Eine Möglichkeit, die Implementierung von Sicherheitsframeworks zu automatisieren, besteht in der Verwendung von Endpoint-Sicherheitslösungen, die die von Ihrem Unternehmen benötigten Frameworks bereits in ihr Tooling integrieren. Das oben erwähnte MITRE ATT&CK-Framework kann beispielsweise in bestimmten Endpoints-Sicherheitslösungen als grundlegende Komponente eingesetzt werden. Auf diese Weise werden die Daten der Verhaltensanalyse bekannten Bedrohungen zugeordnet, die in der MITRE ATT&CK-Datenbank enthalten sind, um die Erkennung zu vereinfachen, und integrierte Workflows zur Risikominderung sind Teil des laufenden Überwachungsprozesses.

Eine andere, ganzheitlichere Methode zur Automatisierung der Compliance durch Sicherheitsframeworks besteht darin, Ihre Mobile Device Management (Mobilgeräteverwaltung, MDM)-Lösung und das mSCP-Framework zu nutzen, um die für die Compliance erforderlichen Dateien zu generieren und sie in Ihre MDM-Lösung hochzuladen, um die Compliance zu automatisieren und durchzusetzen.

BEISPIEL

Durch die Verwendung von mSCP zur Erstellung einer benutzerdefinierten Baseline unter Verwendung des NIST SP 800-53r5-Frameworks als Grundlage zur Erreichung der HIPAA-Konformität mit Endpoints, die in Ihrem MDM registriert sind, kann ein Unternehmen eine Baseline erstellen, die die HIPAA-Anforderungen erfüllt. Ihr nächster Schritt ist die Verwendung von mSCP, um angepasste Dateien zu erstellen:

- **Konfigurationsprofile:** Ermöglicht die Konfiguration von verwalteten Einstellungen, die an die Bedürfnisse Ihres Unternehmens angepasst sind.
- **Skripte zur Einhaltung der Vorschriften:**Zwei Skripte - eines, um verwaltete Geräte auf Sicherheitsanforderungen zu prüfen, und das zweite, um die notwendigen Korrekturen vorzunehmen, um die gewünschte Konformität mit zu erreichen.
- **PLIST-Dateien:** Sie dienen der Überprüfung der Konformität und der Aufzeichnung der Prüfungsergebnisse.
- **Spreadsheet-Dokumente:** Nützlich zur Übergabe an Prüfer und externe Ermittler bei der Feststellung der Einhaltung von Vorschriften.
- **Berichtsdokumente:** HTML- und PDF-basierte Berichte, in denen jede Einstellung, die im Rahmen der Konformitätsprüfung überprüft wird, aufgeführt ist, einschließlich Informationen darüber, was überprüft wird, welche Einstellungen konform sein sollten und wie sie behoben werden können.

Mit diesen Dateien können Administrator*innen alle benutzerdefinierten Konfigurationsprofile (die nicht bereits im MDM vorhanden sind) hochladen, um sie für ihre Flotte bereitzustellen. Das Hochladen der Compliance-Skripte ist jedoch der Punkt, an dem die sprichwörtliche Magie geschieht. Wenn das Auditing-Skript so konfiguriert ist, dass es nach Ihrem Zeitplan, z. B. einmal täglich, ausgeführt wird, wird das Skript für jedes verwaltete Gerät täglich ausgeführt und der Gerätedatensatz im MDM mit neuen Bestandsdaten aktualisiert. Dadurch wird die kritische Erfassung von Telemetriedaten automatisiert, um festzustellen, ob das Gerät die HIPAA-Vorschriften erfüllt. Als Nächstes wird das Abhilfeskript hochgeladen und als Teil einer Richtlinie zur Ausführung gebracht. Auf diese Weise können Administrator*innen den Umfang der Abhilfemaßnahmen so einschränken, dass sie automatisch nur auf den Geräten durchgeführt werden, die die Anforderungen nicht erfüllen. Sobald das Abhilfeskript abgeschlossen ist, löst es eine Bestandsaufnahme der Geräte aus, um die Gerätedatensätze zu aktualisieren und den Status der Konformität im MDM anzuzeigen.

Die Automatisierung der Konformität durch die Integration von Frameworks über Ihre MDM-Lösung ermöglicht die sichere Konfiguration von Geräten, um die Konformitätsziele zu erreichen, und nutzt gleichzeitig Cloud-basierte Verwaltungstools, um die Sicherheit und den Datenschutz Ihrer Endpoints durchzusetzen. Sollte ein Gerät aus dem Geltungsbereich fallen, ermitteln die automatisierten Skripte, welche Einstellung(en) betroffen sind, und beheben das Problem - jederzeit, an jedem Ort und über jede Netzwerkverbindung - ohne dass IT- oder Sicherheitsteams das Gerät physisch anfassen müssen. Durch die Integration Ihrer MDM- und Endpointsicherheitslösungen über eine sichere API-Verbindung werden ständige Transparenz und Überwachung gemeinsam genutzt. Sie unterstützt die Erstellung fortschrittlicher Workflows, die eine schnellere Reaktion auf Vorfälle ermöglichen, einschließlich der SOAR-ähnlichen Technologie (Security Orchestration, Automation and Response), um die Koordination von Ausführungs- und Abhilfemaßnahmen zu automatisieren.

WAS EIN SICHERHEITSFRAMEWORKS LEISTEN KANN UND WAS NICHT

Frameworks eignen sich hervorragend für die Behandlung einer Vielzahl von Themen. Wir haben besprochen, was Frameworks sind (und was nicht). Als Nächstes nehmen wir uns einen Moment Zeit, um zu erörtern, was sie können und was sie nicht können.

Dose

- Strukturierung der Konformitätsanforderungen in geordnete Gruppen von Kategorien
- Formatierung von Details zur Schadensbegrenzung mit Unterstützung für bewährte Praktiken und Methoden der Branche
- als Blaupause für Organisationen dienen, die sich auf dem Weg zur Einhaltung der Vorschriften befinden
- Schaffung einer soliden Grundlage für die Einführung eines umfassenden Cybersicherheitsprogramms

Kann nicht

- Schutz von Organisationen vor Risiken oder Verbindlichkeiten, die sich aus geminderten oder nicht geminderten Risiken ergeben
- freiwillig sein, d. h. es gibt kein Mandat, es ganz oder teilweise umzusetzen
- Verschreiben Sie ausdrücklich die Einhaltung der Lösung. Viele auf der Einhaltung von Vorschriften basierende Frameworks, wie z. B. HIPAA, sind nicht präskriptiv, d. h. sie enthalten keine expliziten Anforderungen, wie die Einhaltung von Vorschriften am besten umzusetzen ist
- Selbst für Schutz sorgen. Sie bieten lediglich Anhaltspunkte dafür, wie ein umfassender Sicherheitsplan aussehen sollte
- Begrenzen Sie die Zeitspanne zwischen den Aktualisierungen. Dies könnte dazu führen, dass einige Informationen bestenfalls veraltet und schlimmstenfalls völlig unrealistisch sind, wenn man die moderne Bedrohungslandschaft betrachtet.
- Neben den Sicherheitskontrollen einbezogen werden - da sie außerhalb eines Defense-in-Depth -Plans für die Sicherheit oder die Einhaltung der Vorschriften nicht ausreichen
- Sicherstellung eines einheitlichen Standes der Einhaltung der Vorschriften. Im Bereich der Sicherheit gibt es keine Patentrezepte, was auch für Frameworks gilt. Nur weil Ihr Unternehmen heute die Vorschriften einhält, heißt das nicht, dass dies auch morgen noch gewährleistet ist.

DER WERT VON APPLES NATIVEN SICHERHEITSFRA-MEWORKS

Was viele nicht wissen: Apple entwickelt eine eigene Reihe von Sicherheitsframeworks - Apple Platform Security -, die jedes Betriebssystem unterstützen und mit anderen datenschutzfreundlichen Frameworks zusammenarbeiten, um die gesamte Apple Produktpalette zu schützen.

Sie erstrecken sich von der Hardware bis zur Software, einschließlich der Art und Weise, wie die physische Sicherheit und die Datensicherheit verarbeitet, gehandhabt, gespeichert, übertragen und von den Nutzer*innen auf den Apple Geräten abgerufen wird. Und was den Datenschutz betrifft, so hat Apple den Rahmen für die App-Tracking-Transparenz entwickelt, mit dem kontrolliert wird, wie Apps Daten über Endnutzer sammeln und weitergeben, um zu begrenzen, was erlaubt ist, und gleichzeitig einzuschränken, was nicht erlaubt ist, um das Recht der Nutzer*innen auf Privatsphäre zu wahren.

Apple ist führend in Sachen Sicherheit und Datenschutz, indem es diese Frameworks entwickelt, sie in seine Betriebssysteme integriert und regelmäßig aktualisiert, um mit den sich entwickelnden Bedrohungen Schritt zu halten, die andernfalls die Informationssicherheit und den Datenschutz der Nutzer*innen gefährden würden.

WAS IST DIE ROLLE VON JAMF?

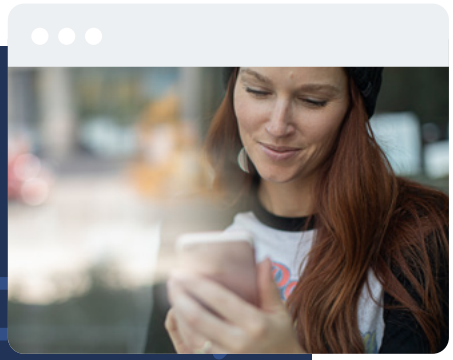
Sie wissen, wie sehr sich Apple für Sicherheit und Datenschutz einsetzt. Aber wussten Sie, dass Jamf Lösungen wie ein IT- und Sicherheitsteam für Ihre IT- und Sicherheitsteams sind?

Nun, das tun wir. Mit unserer langjährigen Erfahrung in der Unterstützung von Apple in Unternehmen bietet Jamf die Lösungen, die Unternehmen zum Erfolg mit Apple verhelfen. Ob bei der Arbeit, in der Schule oder in der Freizeit - Jamf ergänzt die von Apple entwickelten nativen Frameworks, indem es Einblick in diese Frameworks gewährt und so die Antworten auf die Fragen liefert, die Sicherheitsexpert*innen über ihre Apple Flotte stellen sollten:

- Wie sind sie konfiguriert?
- Wann werden sie eingesetzt?
- Warum wurde auf diese Ressource zugegriffen?
- Wer greift darauf zu?
- Werden die Geräte sicher verwendet?
- Was kann sie weiter absichern?
- Wie kann die Einhaltung der Vorschriften gemessen werden?
- Was ist erforderlich, um die Einhaltung der Vorschriften durchzusetzen?

Aber das ist noch nicht alles.

JAMF HILFT IHNEN, DIE THEORIE IN DIE PRAXIS UMZUSETZEN



Frameworks allein tragen nicht zur Sicherheit bei. Umfangreiche Telemetriedaten können einen Einblick in den Zustand der Endpoints geben, um den Konformitätsstatus zu bestimmen, aber diese Daten müssen verwertbar sein, damit Risiken gemindert und die Konformität durchgesetzt werden können.

Unser Flaggschiff, die MDM-Lösung Jamf Pro, ist nicht nur der Goldstandard in der Verwaltung von Apple Geräten, weil wir das sagen, sondern weil Millionen von verwalteten Geräten weltweit und in allen Branchen das sagen. Jamf hilft Unternehmen jeder Größe, die Basisdaten des Frameworks zusammen mit ihren Risikobewertungsdaten zur Bestimmung der Datensicherheit und der Compliance-Anforderungen in Jamf Pro zu nutzen, um Gerätekonfigurationen zu verwalten, die Angriffsfläche durch Gerätehärtung zu minimieren und Richtlinien zu implementieren, die ihnen nicht nur bei der Einhaltung, sondern auch bei deren Durchsetzung helfen.

Durch eine Kombination aus automatisierten Workflows, die von Jamf Protect gesteuert werden - der besten Endpoint-Sicherheitslösung, die speziell für Apple entwickelt wurde - können IT- und Sicherheitsteams die Sicherheits- und Compliance-Anforderungen schnell erfüllen.

Die Endpointsicherheit von Jamf umfasst die Unterstützung von CIS-Baselines, d. h., egal ob Ihr Unternehmen gerade erst anfängt, sich mit Sicherheit und Compliance zu beschäftigen, oder ob Ihr Team aus erfahrenen Profis besteht - Jamf hilft Unternehmen, ihre Infrastruktur schnell und von Grund auf zu sichern. Nehmen wir an, Sie sind bereit, bei der Einhaltung von Vorschriften und der Sicherheit einen Schritt weiterzugehen. In diesem Fall können Sie mit zusätzlichen Sicherheitsframeworks wie MITRE ATT&CK arbeiten oder komplexere Compliance-Anforderungen mit Unterstützung für NIST- und mSCP-Frameworks erfüllen, um nur einige zu nennen.

Jamf Lösungen auf Apple Geräten bedeuten, dass sich IT- und Sicherheitsteams auf die Unterstützung von Geschäftsinitiativen und die Bereitstellung von erstklassigem Support konzentrieren können, während gleichzeitig sichergestellt wird, dass die sich entwickelnden Sicherheits- und Compliance-Anforderungen des Unternehmens verstanden, behandelt und effizient und effektiv behoben werden.

Überzeugen Sie sich selbst mit einer kostenlosen Testversion oder kontaktieren Sie Ihren bevorzugten Reseller.

Los geht's