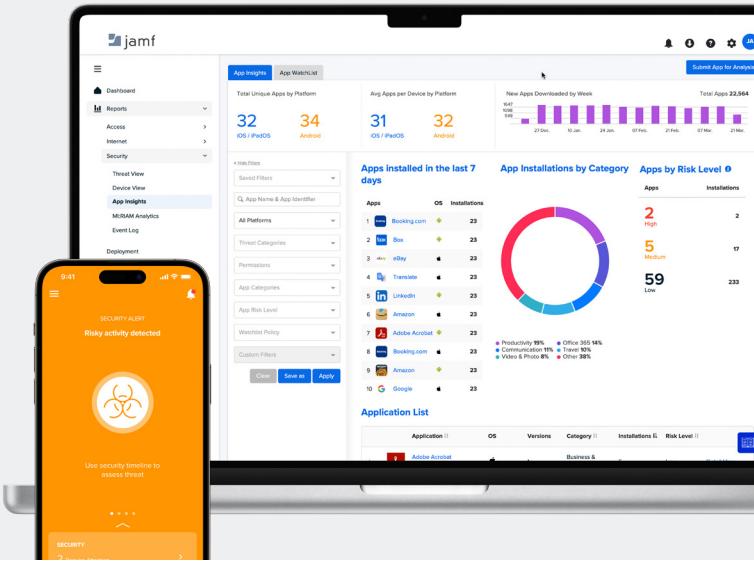
jamf

Best Practices:

Abwehr von Bedrohungen im Unternehmen



Sicherheit bedeutet für verschiedene Unternehmen viele Dinge. Risiken, die in einer Organisation als kritisch eingestuft werden, können in einer anderen Organisation oder Industrie eine geringere Bedeutung haben - nicht, weil erstere die Sicherheit ernster nimmt als letztere - sondern einfach aufgrund der Compliance-Anforderungen, die für jede Organisation und ihre jeweilige Industrie einzigartig sein können.

Abgesehen von den Unterschieden bei der Klassifizierung und Priorisierung von Risikofaktoren zwischen Organisationen gibt es eine Gemeinsamkeit bei den Plänen für Cybersicherheit in allen Unternehmen: Das Ziel ist die Stärkung des Sicherheitsstatus.

Ein Schlüssel zum Erfolg im Unternehmen ist die Ergänzung des Plans für Cybersicherheit durch bewährte Strategien zur Abwehr von Bedrohungen. Die in diesem technischen Dokument vorgestellten Strategien zählen nicht nur einzeln angewandt zu den branchenweit anerkannten Best Practices, um die Vertraulichkeit, Integrität und Verfügbarkeit von Endpoints und sensiblen Daten sicherzustellen. In Kombination entfalten sie ihr volles Potenzial und ermöglichen es Organisationen, durch die Umsetzung der in diesem Leitfaden beschriebenen Lösungen von folgenden Vorteilen zu profitieren

- Entwicklung einer umfassenden Verteidigungsstrategie
- Ausweitung des Schutzes auf Ihre gesamte Infrastruktur
- Streamline Mac- und Mobil-Endpoint-Verwaltung und -Schutz
- Compliance bei der Datensicherheit sowie der Privatsphäre von Benutzer*innen aufrechterhalten
- Minimierung der Komplexität durch Konsolidierung von IT- und Sicherheits-Workflows
- Beschleunigung der Reaktion auf Vorfälle mit gleichzeitiger Erhöhung der Benutzerproduktivität und des ROI.

1. Verschlüsselung der Daten

Wir beginnen unsere Zusammenstellung mit Verschlüsselung. Die Verschlüsselung des Volumens auf allen Geräten wird zwar oft als letzte Verteidigungslinie bezeichnet, bietet aber einen Schutz vor unbefugtem Zugang durch Angreifer, falls andere Verteidigungslinien Angriffe nicht verhindern können. Die Algorithmen, die die Verschlüsselung vornehmen, mögen komplex sein, aber zum Glück für Administrator*innen ist die Bereitstellung der Sicherheitsfunktion einfach und leicht zu handhaben, wenn sie über Ihre MDM-Lösung (Mobile Device Management) bereitgestellt wird.

Administrative Workflows enthalten Checklisten mit Best Practices. Das Einrichten eines Administratorkontos und -passworts für alle von der IT verwalteten Geräte, die Verwaltung von Benutzerberechtigungen zum Entsperren verschlüsselter Datenträger sowie die präzise Dokumentation der Wiederherstellungsschlüssel jedes einzelnen Geräts sind wichtige Aufgaben zum Schutz vor unbefugtem Datenzugriff. Aufgrund ihrer Komplexität und des hohen manuellen Aufwands bringen sie jedoch zusätzlichen Verwaltungsaufwand mit sich und erhöhen das Risiko für Fehler im Prozess. Die Vielfalt der unterstützten Betriebssysteme (OS), multipliziert mit der Anzahl der Geräte, stellt eine große Herausforderung dar, diese wichtigen Informationen stets aktuell und korrekt zu verwalten.

Die Aktivierung der Volumen-Verschlüsselung über Ihre MDM-Lösung vereinfacht die Bereitstellung von Datenverschlüsselungs-Workflows auf Geräten, indem:

- eine einheitliche Durchsetzung in allen Apple Geräteflotten mit macOS, iOS, iPadOS, watchOS, tvOS und visionOS gewährleistet wird.
- Gleiche Sicherheit für unternehmenseigene und BYO-Geräte bei gleichzeitiger Wahrung der Privatsphäre der Benutzer*innen erreicht wird.
- Verschlüsselungs-Workflows automatisiert werden und nahtlosen Schutz ab dem Zeitpunkt erzwungen wird, an dem die Geräte das Verfahren beim Onboarding abschließen.
- Admin-Konten auf hoher Ebene werden nach erfolgreicher Registrierung erstellt werden, wobei die Local Administrator Password Solution (LAPS) für Jamf Pro genutzt wird, um zufällige Passwörter für verwaltete lokale Admin-Konten zu speichern, regelmäßig zu ändern und anzuzeigen
- Zentrale Verwaltung von Wiederherstellungsschlüsseln in einem eindeutigen Datensatz eines Geräts zur sicheren Speicherung und zum einfachen Zugang bei Bedarf.

2. Regelmäßige Patches und Updates

Eine der effektivsten Möglichkeiten für Organisationen, ihre Geräte, Benutzer und Daten zu schützen, besteht darin, ihre Geräte mit Sicherheitsupdates sowie System- und Anwendungspatches auf dem neuesten Stand zu halten. Während Zero-Day-Bedrohungen sowohl in ihrer Häufigkeit als auch in ihrer Auswirkung zugenommen haben, konzentrieren wir uns in diesem Abschnitt auf bekannte Schwachstellen und Bugs, die im Code gefunden wurden und für die bereits Patches/Updates vom Entwickler*in zur Verfügung stehen, um das Problem zu beheben, sowie auf die entscheidende Bedeutung einer regelmäßigen Update-Kadenz für die Aufrechterhaltung des Sicherheitsstatus Ihrer Geräte und Ihres Unternehmens.

Wichtig bei bekannten Schwachstellen ist der Begriff "bekannt", d. h., es gibt ein Update, um das Risiko, das die Schwachstelle für die Daten des Unternehmens und die Compliance-Anforderungen darstellt, zu mindern. Vor diesem Hintergrund gibt es eine Reihe von in MDM eingebauten Methoden, die nicht nur dazu beitragen, Geräte vor bekannten Bedrohungen zu schützen, sondern auch den nativen OS-Sicherheitsschutz zu verstärken, indem sie neue Funktionen und Funktionalitäten freischalten, die oft in den neuesten Updates enthalten sind. Dies bietet Unternehmen Vorteile, indem sie sowohl die Geräte-Sicherheit als auch die Produktivität der Endbenutzer*innen aufrechterhalten.

MDM-Lösungen stellen unter anderem auf flexible Weise sicher, dass Geräte auf dem neuesten Stand bleiben:

- Same Day Support für OS Updates und Upgrade-Workflows bedeutet, dass Organisationen ihre Geräte nach ihrem eigenen Zeitplan patchen können - nicht nach unserem.
- Verwaltete Apps werden immer auf dem neuesten Stand gehalten, wenn sie im Apple App Store bereitgestellt werden. Für Apps von Drittanbietern, bei denen das nicht der Fall ist, automatisiert Jamf App Installers den Aktualisierungsprozess für mehr als 700 Apps im Jamf App-Katalog.
- Halten Sie die Compliance aufrecht, indem Sie die OS-Anforderungen durch richtlinienbasiertes Management durchsetzen.
- Die Integration mit Jamf Connect ermöglicht einen Zero-Trust-Netzwerkzugriff (ZTNA), der geschützte Ressourcen vor gefährdeten Geräten schützt und automatisierte Abhilfeworkflows auslöst.
- Verwaltung und Schutz von Endpoints über eine zentralisierte, ganzheitliche Lösung, die konvergenten Teams den erforderlichen Einblick in die Gesundheit der Geräte mit den erforderlichen Tools bietet, um Aktualisierungen auf der Grundlage von Echtzeit-Telemetriedaten vorzunehmen.

3. Multi-Faktor-Authentifizierung (MFA)

Wenn es um Identitäts- und Zugangsverwaltung (IAM) und Defense-in-Depth-Strategien geht, ist MFA die logische Weiterentwicklung bei der Implementierung von Sicherheitskontrollen, um zu überprüfen, ob Benutzer*innen bei der Authentifizierung die sind, die sie vorgeben zu sein. Die Überprüfung von Anmeldeinformationen ist die eine Hälfte des Zero-Trust-Modells. Die alte Methode, sich ausschließlich auf Anmeldeinformationen der Benutzer*innen zu verlassen, um den Zugang zu sensiblen Ressourcen zu beschränken, hat sich als unwirksam erwiesen, wenn Passwörter leicht zu erraten sind oder der minimale Schutz, der geboten wird, von Bedrohungsakteuren, die mühelos Anmeldeinformationen aus sehr erfolgreichen Angriffen wie Phishing-Kampagnen abgreifen, vollständig umgangen wird.

Laut der Cybersecurity and Infrastructure Agency [Agentur für Cybersicherheit und Infrastruktur] (CISA) "ist die Wahrscheinlichkeit, gehackt zu werden, durch die Verwendung von MFA für Ihre Accounts um 99 % geringer". Diese Statistik wird von Organisationen wie Microsoft und Google bestätigt, die 99,9 % der Angriffe auf Ihre Accounts verhindern bzw. rund 99,9 % der automatisierten Bot-Angriffe blockieren. Dies unterstreicht, wie wichtig MFA für Ihre Sicherheit ist, aber auch, dass es wichtig ist, dafür sorgen, dass:

- das gleiche Sicherheitsniveau auf alle Endpoints erweitert wird, unabhängig von ihrem Besitzmodell oder davon, ob die Benutzer*innen als Teil einer verteilten Arbeitskraft oder vom Büro aus arbeiten.
- Bedrohungen, die auf Anmeldeinformationen basieren, minimiert werden und der unbefugte Zugang zu geschützten Ressourcen verhindert wird - selbst im Falle von gefährdeten Passwörtern.
- Integration neben anderen Kontrollen, Funktionen und Services als zusätzliche Verteidigungsschicht gegen moderne Bedrohungen gewährleistet wird.
- das Risiko der Authentifizierung vermindert wird, indem Sie passwortlose Workflows implementieren, die leicht zu erratende Passwörter durch zwei oder mehr Verifizierungsfaktoren ersetzen, die nur schwer zu umgehen sind.
- die Benutzererfahrung bei der Bereitstellung von Geräten oder beim Zugang zu Unternehmensressourcen vereinfacht wird, indem Sie die Authentifizierung durch Single Sign-On (SSO) und passwortlose Sicherheit mit nur einem mobilen Gerät automatisieren.

4. Zero-Trust Architektur

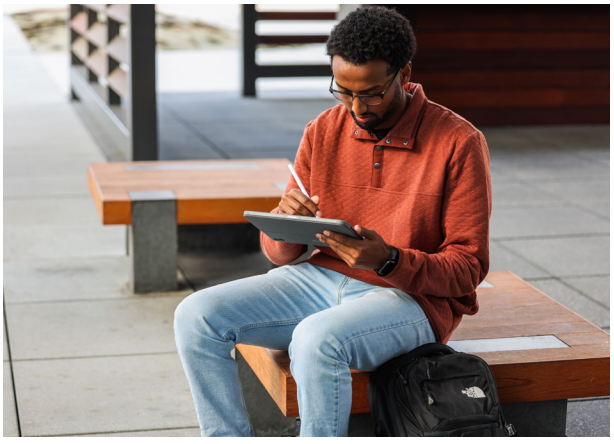
Was die entscheidende Rolle der Identitätsintegration innerhalb Ihres Sicherheitsstapels betrifft, so ist keine Diskussion vollständig ohne Zero-Trust-Netzwerkzugriff und die Art und Weise, wie das auf Zero-Trust basierende Modell die nächste Generation von IAM anwendet, um den Zugang nur auf verifizierte Benutzer*innen und konforme Geräte einzuschränken - alle anderen werden standardmäßig verweigert.

Die moderne Bedrohungslandschaft spiegelt die aktuelle Computer-Landschaft insofern wider, als diese die Art und Weise, wie die Arbeit im Unternehmen ausgeführt wird, verändert hat. Ob im Büro oder als Teil einer verteilten Arbeitskraft, auf einem Mac Computer oder einem mobilen Gerät, das persönlich oder unternehmenseigen sein kann - die Produktivität muss von jedem Gerät, zu jeder Zeit, von jedem Ort und über jede sichere Netzwerkverbindung erfolgen.

Genauso wie Organisationen sich an hybride Arbeitsumgebungen anpassen müssen, muss sich auch die Sicherheit weiterentwickeln, damit Geräte, Benutzer*innen, Daten und die Netzwerkverbindungen, über die sie kommunizieren, trotz der vielen Herausforderungen und Bedrohungen sicher bleiben, wie z. B. der Anstieg der weltweiten Cyberangriffe auf Mobilgeräte **um 147 %** zwischen Dezember 2022 und 2023.

ZTNA trägt unter anderem dazu bei, Bedrohungen durch Macs und mobile OS im Unternehmen zu verhindern:

- Geräte, Daten und Ressourcen sind geschützt, aber getrennt. Das bedeutet, dass jede Ressourcen-Anfrage standardmäßig verweigert wird, bis die Gesundheit des Geräts überprüft wurde. Dadurch wird die Sicherheit der Daten gewährleistet, indem sichergestellt wird, dass die Anmeldeinformationen nicht kompromittiert wurden und die Geräte konform sind, bevor der Zugang gewährt wird.
- Eine Cloud-basierte Infrastruktur ermöglicht die einfache Integration und Erweiterung einer konsistenten Bedrohungsabwehr für Desktop- und mobile Flotten, ohne dass komplexe Geräte oder Konfigurationen verwaltet werden müssen, und optimiert die Sicherheit unabhängig vom Betriebssystem, Gerätetyp oder Eigentumsmodell der für die Arbeit verwendeten Geräte.
- Sichern Sie alle Netzwerkverbindungen durch Mikrotunneling, das jede Anfrage isoliert, um netzwerkbasierte Bedrohungen wie Man-in-the-Middle-Angriffe zu verhindern, und halten Sie sich dabei an das Prinzip der geringsten Privilegien, indem Sie nur verschlüsselten Zugriff auf die Ressourcen gewähren, für die die Nutzer*innen eine Zugangsberechtigung haben (im Gegensatz zu herkömmlichen VPN-Lösungen, die impliziten Zugriff auf Ihr gesamtes Netzwerk bieten).
- Nutzen Sie kontextbasierte Richtlinien für den Zugang, um die Einhaltung von Unternehmens- und/oder gesetzlichen Vorschriften zu erzwingen oder den Zugang auf der Grundlage von Anforderungsnachweisen, wie z. B. OS/App-Patch-Stufen, zu erlauben/zu verweigern.
- Der Always-on-Schutz gewährleistet, dass Geschäftsdaten sicher bleiben, während Split-Tunneling personenbezogene Daten auf intelligente Weise direkt ins Internet leitet. Wahrung der Privatsphäre der Benutzer*innen ohne Beeinträchtigung der Sicherheit oder umgekehrt.



5. Schwachstellenanalyse

Auch auf die Gefahr hin, dass es so klingt, als würden wir die Bedeutung aufbauschen, sind Risikobewertungen im Bereich der IT- und Informationssicherheit von größter Bedeutung. Angefangen bei der Tatsache, dass man nicht erwarten kann, etwas sicher aufzubewahren, wenn man nicht herausgefunden hat, was dieses "Etwas" ist. Im Rahmen eines Programms zur Verwaltung von Schwachstellen ist das Verfahren zur Bewertung der Risiken und Schwachstellen, die Ihre Organisation betreffen, ein entscheidender erster Schritt, der jeden weiteren Teil des Prozesses beeinflusst. Letzten Endes ist er die Grundlage für jede Kontrolle, jedes Verfahren und jeden Workflow auf jeder Ebene eines umfassenden Cybersicherheitsplans, der in die Tiefe geht.

Das Verfahren zum Management von Schwachstellen umfasst fünf Phasen, wobei wir uns in diesem Abschnitt auf die ersten beiden konzentrieren:

1. Identifizierung
2. Bewertung
3. Prioritätensetzung
4. Auflösung
5. Berichterstattung

Wir haben bereits darauf hingewiesen, warum die Identifizierung so wichtig ist - man kann nicht schützen, was man nicht kennt. Bei einer MDM-Lösung beginnt dieses Verfahren mit Ihrem Bestand, um die Geräte und alle relevanten Variablen zu ermitteln, die sich auf Ihren Sicherheitsstatus auswirken könnten. Einige Beispiele sind:

- Gerätetyp
- Betriebssystemversion
- Installierte Apps
- Härtungskonfigurationen
- Installierte Endpoint-Schutz Software
- Eigentumsmodell
- Zugewiesene Benutzer*innen

Die nächste Stufe, die Bewertung, beruht auf der Fähigkeit Ihrer Endpoint-Schutz-Lösung, den Gesundheitszustand jedes Geräts, das mit Ihrer Infrastruktur in Berührung kommt, zu bestimmen. Durch die Kombination von Geräte-Scans, Protokolldaten und dem von Ihrem MDM freigegebenen Bestand können Admins mit diesen Telemetriedaten die aktuelle Gesundheit der Endpoints in Echtzeit mit den Basisdaten vergleichen, um beispielsweise festzustellen, ob Sicherheitslücken bestehen, weil:

- Betriebssysteme nicht auf die neueste Version aktualisiert werden
- Installierte Apps von bekannten Schwachstellen betroffen sind
- Bei den Geräten Sicherheitskonfigurationen fehlen oder sie falsch konfiguriert sind
- Netzwerk-Verbindungen auf dem Gerät eines Fernbenutzers*in unsicher sind

6. Mac Endpoint Erkennung und Reaktion (EDR):

Wenn das Risiko identifiziert und bewertet ist, folgen als Nächstes die letzten drei Phasen des Schwachstellen-Managements, in denen es darum geht, aus der Sammlung und Analyse von Daten Aufgaben zu entwickeln, die Bedrohungen eindämmen, bevor sie sich weiter ausbreiten.

Die dritte Stufe ist die Prioritätensetzung. Hier sortieren Admins und/oder eine mit künstlicher Intelligenz (KI) angereicherte Software für Endpoint-Schutz die Ergebnisse in Klassifizierungen für Schwachstellen und Risikofaktoren, um die Auswirkungen im Unternehmen zu bestimmen.

Die vierte Stufe, die Behebung, trägt ihren Namen zu Recht, denn hier stellen IT-/Sicherheitsteams Workflows zur Behebung von Schwachstellen bereit, die in den vorangegangenen Stufen erkannt wurden, wobei sie in dieser Phase vom höchsten bis zum niedrigsten Schweregrad vorgehen.

Der letzte, aber sehr wichtige Teil des Verfahrens zur Verwaltung von Schwachstellen ist die Berichterstattung. In dieser Phase arbeiten die Teams daran:

- alle Ergebnisse (d. h. was passiert ist) zu dokumentieren.
- positive und negative Ergebnisse (d.h. was hat funktioniert, was nicht) zu vermerken.
- Feedback zu geben, um aktuelle und künftige Workflows zu informieren (d.h. die Hauptursache, warum etwas nicht funktioniert hat oder welche Probleme, wenn überhaupt, aufgetreten sind).
- die Verfahren zu verbessern, indem Sie die gewonnenen Lektionen überprüfen (d. h. Dinge, auf die Sie achten sollten und die das Verfahren in Zukunft besser/einfacher/weniger fehleranfällig machen würden).

Als Teil einer Defense-in-Depth-Strategie ist EDR in der Lage, durch die sichere Integration mehrerer Lösungen Cyber-Erfolge zu erzielen, um:

- Endpoints aktiv auf mehrere Risiken zu überwachen und Teams bei erkannten Problemen wie Malware oder Nichteinhaltung von Vorschriften zu alarmieren.
- Telemetriedaten manuell oder mithilfe von KI zu analysieren, um bekannte und unbekannte Bedrohungen zu identifizieren.
- Threat Prevention zu automatisieren oder betroffene Geräte bis zur weiteren Überprüfung unter Quarantäne zu stellen.
- Bedrohungen zu entschärfen, indem Sie die betroffenen Endpoints bereinigen und automatisch Workflows zur Behebung auslösen.
- Proaktiv vor Bedrohungen zu schützen, indem maschinelles Lernen (ML) eingesetzt wird, um Bedrohungssuche durch schnelles Sammeln und Analysieren von Threat Intelligence zu betreiben. Außerdem werden die Reaktionszeiten verkürzt und die Teams beraten, wie sie reagieren sollen.

7. KI-gesteuerte Threat Intelligence

KI- und ML-gesteuerte Lösungen helfen Teams jeder Größe - nicht nur solchen mit engagierten IT-/Sicherheitsexperten - Daten zu sammeln, zu analysieren und datengesteuerte Entscheidungen schneller zu treffen, als dies mit manuellen Verfahren möglich ist. Und Zeit ist sozusagen nur die Spitze des Eisbergs, wenn es um die Einsparungen und den ROI geht, die KI/ML Organisationen bringt.

Laut IBM„verbessert die KI ihr Wissen, um Cybersicherheits-Bedrohungen und Cyberrisiken zu „verstehen", indem sie Milliarden von Datenartefakten nutzt" Dies ist die zentrale Komponente, die es Organisationen ermöglicht, durch die Integration von KI/ML in ihre Cybersicherheitsstrategie von den folgenden Vorteilen zu profitieren:

- Zusammenarbeit mit Administrator*innen, um die Daten zu erhalten, die Sie benötigen, um fundierte Entscheidungen in Bezug auf Bedrohungen zu treffen, und zwar auf der Grundlage maßgeschneiderter Threat Intelligence, die auf Ihre individuelle Umgebung zugeschnitten ist.
- Überwachung, Identifizierung, Erforschung, Ausnutzen, Überprüfung und Behebung unbekannter Bedrohungen 24x7x365 sowie Entwickeln von Bedrohungsmodellen auf der Grundlage logischer und empirischer Datenpunkte.
- Proaktives Erkennen und Stoppen von Bedrohungen, bevor sie eskalieren, kann den ROI erhöhen und Geld für die Beseitigung kostspieliger Datenverletzungen (und Compliance-bedingter Nachwirkungen) sparen.
- Schnelleres Reagieren auf Vorfälle und Beschleunigung der Lösungszeiten, indem Sie das Zeitfenster zwischen der Erkennung von Bedrohungen und der Behebung von Problemen verkleinern.
- Nutzung von ML und automatisierten Sicherheits-Workflows, um Ihre IT/Sec-Teams zu befähigen, sich auf die Entwicklung besserer Technologien zu konzentrieren, die den Stakeholdern helfen, intelligenter und nicht härter zu arbeiten.

8. Richtlinien für die Geräte-Compliance

Eine Schlüsselkomponente der Compliance sind die Konfigurationen der Geräte, die dazu dienen, die Angriffsfläche der Hardware und der auf den Geräten selbst laufenden Software zu verringern. Das Konzept der Härtung besteht darin, Endpoints effektiv "abzuschotten", indem alles entfernt wird, was für die Benutzer*in nicht notwendig ist, um die Aufgaben ihrer Rolle zu erfüllen. Weniger laufender Code bedeutet eine Verringerung der Risikovektoren, die ausgenutzt werden können.

Frameworks sind ausgezeichnete Richtlinien für Organisationen, um die Sicherheit ihrer Geräte, Daten, Services, Verfahren und Workflows zu maximieren. Nach der Konfiguration können jedoch externe Faktoren wie Updates, Malware, neu installierte Apps und risikoreiches Verhalten der Benutzer*innen dazu führen, dass bestehende Einstellungen geändert werden und die Geräte nicht mehr der Compliance entsprechen.

Wenn das Konfigurieren von Einstellungen die eine Hälfte einer Sicherheitslösung für Compliance ist, dann ist die Durchsetzung - durch Richtlinien, die in Ihren MDM-, Identitäts- und Sicherheitslösungen eingerichtet sind - die andere Hälfte.

Richtlinien unterstützen den Sicherheitsstatus einer Organisation auf verschiedene Weise:

- Sie ermöglichen die Durchsetzung von Compliance-Baselines, damit die Geräte den gesetzlichen Anforderungen der Industrie entsprechen.
- Sie können sich vergewissern, dass die Geräte die neueste Version von macOS verwenden oder die Apps für die Produktivität auf dem neuesten Stand sind, um bekannte Schwachstellen zu vermeiden.
- Identitätsprovider (IdP) und Sicherheitslösungen müssen Anmeldeinformationen und/oder Daten zur Gesundheit von Geräten überprüfen, wenn Benutzer*innen den Zugang zu geschützten Ressourcen anfordern, um den Zugang zu kompromittierten Accounts zu verhindern und Geräte zu reparieren, die nicht den Sicherheitsgrundsätzen entsprechen.
- Sie können die Einhaltung der organisatorischen Sicherheitsrichtlinien auf BYO-Geräten sicherstellen, indem sensible Daten und Apps bei der Registrierung automatisch in einem separaten geschäftlichen Bereich isoliert werden, während persönliche Daten und Apps privat bleiben.
- Sie können die Verschlüsselung aller drahtgebundenen und drahtlosen Konnektivitäten erzwingen, wenn sich Fernbenutzer*innen mit nicht registrierten Netzwerken verbinden, um die Sicherheit der Daten zu gewährleisten.

9. Schulungen zum Sicherheitsbewusstsein

Keine umfassende Cybersicherheitsstrategie ist vollständig ohne ein Programm für Schulungen zum Sicherheitsbewusstsein für Endbenutzer *innen.

Laut Forbes "hatten 93 % der Organisationen im vergangenen Jahr zwei oder mehr identitätsbezogene Verstöße". Dazu passt eine Feststellung von Statista, wonach die Zahl der weltweit erkannten Phishing-Seiten allein im ersten Quartal 2024 bei 963.994 lag. Dies verdeutlicht, dass Bedrohungsakteure die mangelnden Sicherheitskenntnisse der Benutzer*innen gezielt ausnutzen, um Identitäten zu kompromittieren und die Reichweite eines Angriffs zu vergrößern.

Das Ziel der Cybersicherheit besteht darin, das Risiko für Ihr Unternehmen so weit zu reduzieren, wie es Ihre Risikobereitschaft zulässt. In diesem Sinne sind Sicherheitsschulungen ein ergänzender Bestandteil Ihrer übergreifenden Sicherheitsstrategie, damit Sie:

- die Benutzer*innen über die neuesten Bedrohungen, die Ihre Organisation betreffen, informieren können.
- häufige Bedrohungen besser erkennbar machen können, damit die Benutzer*innen ihnen weniger leicht zum Opfer fallen.
- Fehler minimieren können, indem Sie das schwächste Glied in der Sicherheitskette stärken: den Menschen.
- Benutzer*innen dazu befähigen können, ihren Teil zum Schutz von Geräten und sensiblen Informationen beizutragen, indem sie Datenlecks einschränken.

  Verbessern Sie die Compliance ganzheitlich, indem sichergestellt wird, dass Benutzer*innen verstehen, was von ihnen erwartet wird, und dass Organisationen sich an die strengen Richtlinien zur Rechenschaftspflicht halten, die in ihren Richtlinien festgelegt sind.

10. Pläne für die Reaktion auf Zwischenfälle

Wir haben uns mit Best Practices befasst, die unabhängig voneinander funktionieren können, aber wenn sie kombiniert werden, wird Ihr Sicherheitsplan durch die Überlagerung der einzelnen Sicherheitskontrollen, Verfahren und Workflows zu einer robusten, umfassenderen Strategie, die Bedrohungen abfängt, bevor sie ausgenutzt werden können.

Doch was passiert, wenn ein Gerät dennoch kompromittiert wird? Laut dem Nationalen Institut für Normen und Technologie (NIST) ist ein solider Plan für die Reaktion auf Vorfälle, der in Ihre Cybersicherheitsstrategie integriert ist, ein entscheidendes Element, um Bedrohungen so schnell wie möglich zu entschärfen.

Ein Plan für die Reaktion auf Vorfälle besteht im Wesentlichen aus vier Schritten:

1. Vorbereitung

- Richten Sie Hardware-/Software-Konfigurationen an Sicherheitsgrundlagen aus, um das Risiko der Nichteinhaltung von Compliance-Vorschriften (Datenverschlüsselung) zu minimieren.
- Integrieren Sie MDM- und Endpoint-Schutz-Lösungen, um Risikobewertungen zu vereinfachen und das Security Management mit einem aktuellen Bestand (Schwachstellen-Bewertung) zu optimieren.

2. Erkennung und Analyse

- Sammeln Sie umfangreiche forensische Daten, um sich ein vollständiges Bild davon zu machen, was passiert ist und, ebenso wichtig, wie der Vorfall abgelaufen ist (EDR).
- Reduzieren Sie die Zeit für die Sammlung und Analyse von Daten von Tagen oder Wochen auf Minuten, indem Sie redundante Sicherheitsaufgaben mit KI/ML-Technologien automatisieren (KI-gesteuerte Threat Intelligence).

3. Eindämmung, Ausrottung und Wiederherstellung

- Minimieren Sie Risikofaktoren und beheben Sie Vorfälle schnell mit orchestrierten Workflows zur Behebung, indem Sie Telemetriedaten sicher zwischen MDM und Endpoint-Schutz austauschen (regelmäßige Patches und Updates).
- Das Erfordernis zusätzlicher Faktoren für die Authentifizierung bietet ein digitales Sicherheitsnetz, das verhindert, dass Daten in die Hände von Bedrohungsakteuren gelangen, falls Anmeldeinformationen kompromittiert werden (MFA).
- Sorgen Sie zudem dafür, dass Benutzer*innen von jedem Gerät aus sicher und produktiv arbeiten können, unabhängig davon, ob es sich um ein persönliches oder ein unternehmenseigenes Gerät handelt, und setzen Sie die Sicherheit in Ihrer gesamten Infrastruktur auf macOS, iOS/iPadOS, tvOS, watchOS, visionOS, Windows und Android Geräten konsequent durch (Zero-Trust-Architektur).

4. Aktivitäten nach einem Vorfall

- Stellen Sie Konfigurationen bereit für die Gerätehärtung zur Durchsetzung der Compliance durch richtlinienbasierte Verwaltungsworkflows für eine einfache und effektive Compliance-Verwaltung (Richtlinien für die Geräte-Compliance).
- Minimieren Sie die Bedrohung durch Bildung und regelmäßige Schulungen, um die Informationen zu stärken, auf die sich Benutzer*innen verlassen können, um häufige Angriffe wie Phishing zu erkennen (Schulungen zum Sicherheitsbewusstsein).

Schlussfolgerung

Testen Sie Ihre Backup-Pläne nicht erst, wenn Sie versuchen, Daten nach einer Katastrophe wiederherzustellen. Das Gleiche gilt für Pläne zur Cybersicherheit.

Ganz gleich, ob Sie ein kleines oder mittelständisches Unternehmen sind, das mit Apple-Geräten arbeitet, eine Bildungseinrichtung, die 1:1 iPad-Programme für sicheres und privates Lernen einsetzt, oder ein Fortune-500-Unternehmen mit Tausenden von Benutzer*innen und Geräten, die eine Mischung aus macOS/iOS, Windows und Android verwenden – jetzt ist der ideale Zeitpunkt, um Ihre Sicherheitsanforderungen zu erfüllen. Setzen Sie auf eine umfassende Verteidigungsstrategie, um Geräte, Nutzer und Daten vor zunehmenden und immer ausgefeilteren Bedrohungen sowie Angreifern zu schützen, die es auf die sensiblen und vertraulichen Informationen Ihres Unternehmens abgesehen haben.

jamf

www.jamf.com/de/

© 2025 Jamf, LLC. Alle Rechte vorbehalten.

Erste Schritte mit Jamf

oder kontaktieren Sie Ihren bevorzugten Reseller, um loszulegen.