jamf

Krisenkontrolle

Schließen von Sicherheitslücken durch Reaktion auf Vorfälle und Wiederherstellung

„Die Reaktion auf Computersicherheitsvorfälle ist zu einem wichtigen Bestandteil von Informationstechnologie (IT)-Programmen geworden. Da eine wirksame Reaktion auf Zwischenfälle ein komplexes Unterfangen ist, erfordert der Aufbau einer erfolgreichen Reaktionsfähigkeit auf Zwischenfälle umfangreiche Planung und Ressourcen

Der Auszug aus dem National Institute of Standards and Technology (NIST) unterstreicht die Notwendigkeit eines soliden Plans für den Umgang mit Sicherheitsvorfällen. Eine rasche, gezielte Reaktion trägt zur Risikokontrolle bei, indem sie die potenzielle Gefährdung begrenzt. Die Sanierungsphase, die durch die verfügbaren Instrumente bestimmt wird, ist sehr unterschiedlich.

Es gibt Lücken.

In diesem Papier befassen wir uns damit:

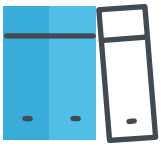
- Was wir aus den fünf Schritten der Reaktion auf Vorfälle - Vorbereitung, Erkennung, Meldung, Reaktion und Behebung - über den Aufbau robusterer Sicherheitsstrategien zur effizienten Bewältigung und Behebung von Bedrohungen lernen können
- Wie man effektive, robuste Playbooks entwickelt, um auf verschiedene Bedrohungen reagieren zu können
- Warum das Verständnis des Wertes von Vermögenswerten und die Einschätzung des Bedrohungspotenzials von entscheidender Bedeutung sind, um erfolgreich auf Sicherheitsbedrohungen zu reagieren und sich davon zu erholen
- Warum ein integriertes Verwaltungs- und Sicherheitskonzept mit einer speziell entwickelten Sicherheitslösung der richtige Weg ist, um Ihre Apple Flotte zu schützen

I. Vorbereitung

Richten Sie Ihr Umfeld für den Erfolg ein.

Benjamin Franklins Sprichwort „Eine Unze Prävention ist mehr wert als ein Pfund Heilung“ klingt heute noch genauso wahr wie damals. Und diese Botschaft könnte für die IT nicht passender sein - insbesondere für den Schutz vor Cybersecurity-Bedrohungen und -Angriffen.

Geeignete Richtlinien, Mitarbeiter*innen und Tools sind entscheidend für die erfolgreiche Eindämmung von Vorfällen und die rasche und effiziente Beseitigung betroffener Geräte. Auf diese Weise wird auch das Potenzial einer Bedrohung verringert, Systemprozesse zu gefährden oder die Geschäftskontinuität auf sinnvolle Weise zu beeinträchtigen.



Bestand

Wie kann etwas geschützt werden, wenn niemand weiß, dass es existiert? Daher ist es von entscheidender Bedeutung, eine aktuelle Bestandsverwaltung zu führen, um alle Vermögenswerte zu schützen. Es ist eine gute Praxis für Organisationen, diese im Auge zu behalten:

- Welche Geräte, Peripheriegeräte und Ressourcen besitzen sie?
- Wie sind sie konfiguriert?
- Wo befinden sie sich?
- Wem sind sie zugewiesen?
- Welche Zugriffsrechte werden gewährt und wem gegenüber?

Die Antworten auf diese Fragen liefern Unternehmen wichtige Informationen, die sich direkt auf die Sicherheit der für die Arbeit verwendeten Geräte und Ressourcen beziehen.

Die Identifizierung und Inventarisierung der Ausrüstung und ihrer jeweiligen Verwendungszwecke vermittelt ein genaues Bild davon, welche Ausrüstung die Organisation besitzt und wofür sie verwendet wird. Achten Sie darauf, alle wertvollen Dienste einzubeziehen, die diese Geräte bereitstellen, wie z. B. die Identifizierung von öffentlich zugänglichen Servern, die Webinhalte bereitstellen, von mobilen Geräten, die in der Telemedizin eingesetzt werden und medizinische Aufzeichnungen oder private Patientendaten speichern, usw.

Risikobewertung

Nach der Bestandsaufnahme ist die nächste Phase die Bewertung der Risikofaktoren:

- Feststellung, für welche Bedrohungen die Geräte anfällig sind
- Die Wahrscheinlichkeit, dass die Bedrohung ausgenutzt wird
- Was die möglichen Folgen sein könnten
- Wie sich dies auf den Geschäftskontinuitätsplan der Organisation auswirkt

Die Bewertung von Risikofaktoren ist eine komplexe Aufgabe, die eine Fülle von Informationen erfordert, um die Geräte und Ressourcen des Unternehmens genau darzustellen. Es erfordert ein tiefes Verständnis der technischen, sicherheitstechnischen, finanziellen, administrativen und rechtlichen Aspekte, um Geräte und ihre Dienste richtig zu bewerten. Die Risikobewertung erfolgt nicht isoliert, sondern umfasst mehrere Beteiligte, die verschiedene Produkt- oder Dienstleistungsbewertungen in Betracht ziehen, bevor sie eine endgültige Entscheidung treffen.

Nehmen wir als Beispiel einen Webserver. Webserver sind öffentlich zugänglich und anfälliger als Geräte, die hinter Firewalls geschützt sind. Wenn ein Webserver eine Verbindung zu einer Datenbank herstellt, in der Benutzerinformationen gespeichert sind, erhöht sich das Risiko, da er zu einem Tor für persönlich identifizierbare oder vertrauliche Daten wird.

Normen und Vorschriften

Die Kenntnis der Vermögenswerte des Unternehmens und ein Plan für die Reaktion auf Vorfälle sind zwei unterschiedliche, aber miteinander verbundene Aspekte.

Bei Vorfällen im Bereich der Computersicherheit ist ein klar definierter Ablaufplan für Reaktionsprotokolle von entscheidender Bedeutung, der es den CSIRTs (Computer Security Incident Response Teams) ermöglicht, unabhängig von der Größe des Teams oder externen Partnerschaften umgehend zu handeln. Der klare und prägnante Plan hat folgende Ziele:

1. Anpassung der Unternehmensressourcen an die Gesetze und Vorschriften der Branche und Erstellung von Compliance-Baselines.

2. Erkannte Bedrohungen können effizient angegangen werden, bevor sie eskalieren, und bieten den schnellsten Weg zurück zu einem konformen Status.

Die Richtlinien können zwar variieren, aber das NIST skizziert Schlüsselelemente für die Entwicklung von Richtlinien für die Reaktion auf Vorfälle in Unternehmen, einschließlich einer Verpflichtungserklärung, des Zwecks der Richtlinie, des Geltungsbereichs, der Definitionen, der Organisationsstruktur, der Risikobewertung, der Leistungsmetriken und der Berichterstattungsverfahren.

Verfahren zur Reaktion auf Vorfälle

Einige Elemente regeln, wie auf Vorfälle zu reagieren ist, andere beziehen sich auf den Plan zur Reaktion auf Vorfälle, in dem die Beteiligten und die jeweiligen Schritte zur Reaktion auf einen Vorfall aufgeführt sind.

Denken Sie daran, dass jeder eine Rolle zu spielen hat - ganz gleich, ob er selbst Hand anlegt oder hinter den Kulissen das Sagen hat - es ist ganz sicher eine Teamleistung. Der Plan selbst dient als Fahrplan mit einem zielgerichteten und koordinierten Ansatz für die Reaktion auf Vorfälle, der auf den besonderen Anforderungen der Organisation basiert und gleichzeitig die Fähigkeiten und Partnerschaften der Organisation für maximale Effektivität nutzt.

Wie die oben genannten Richtlinien kann und wird der Plan je nach Auftrag, Größe, Struktur und Funktionen der Organisation variieren.

Zu den Schlüsselelementen, die bei der Entwicklung eines erfolgreichen Plans zu berücksichtigen sind, gehören:

- Leitbild
- Strategien und/oder Ziele
- Organisatorischer Ansatz
- Bewährte Kommunikationsprozesse
- Metriken zur Messung der Wirksamkeit
- Prozess zur Optimierung der Fähigkeiten
- Integration in die Prozesse der Organisation

Administrative Erwägungen

Zu diesem Zeitpunkt sollte die Organisation entweder ein Team zusammengestellt haben oder eine klare Vorstellung von den geeigneten Personen und ihren Rollen im Modell für die Reaktion auf Vorfälle haben, wobei die Informationen aus früheren Abschnitten zusammengefasst werden. So sind beispielsweise Mitarbeiter*innen der IT- und Informationssicherheitsabteilung aufgrund ihrer umfassenden Infrastrukturkenntnisse ideal für das Reaktionsteam. Darüber hinaus sind Personen mit Erfahrung im Projektmanagement unerlässlich, um den Sanierungsprozess durch effiziente Organisation und Planung der erforderlichen Ressourcen zu beschleunigen. Der Ansatz ist unterschiedlich: Größere Unternehmen verfügen in der Regel über eigene interne Teams für die Behandlung von Sicherheitsfragen, während kleinere Unternehmen dazu angehalten sind, bei der Reaktion auf Vorfälle mit externen Anbieter*innen zusammenzuarbeiten und deren besondere Stärken zu nutzen.

Der Aufbau von Partnerschaften ist nicht auf kleinere Organisationen beschränkt; größere, engagierte Teams arbeiten oft mit Anbieter*innen, Strafverfolgungsbehörden und Einrichtungen wie dem United States Computer Emergency Readiness Team (US-CERT) in den USA zusammen, um die Reaktion auf Vorfälle zu koordinieren. Partnerschaften mit Anbieter*innen können nützliche Dienste anbieten, und Unternehmen müssen mit der staatlichen Organisation vertraut sein, die in ihrem Land oder ihrer Region für die Reaktion auf Vorfälle zuständig ist, um zusätzliche Unterstützung zu erhalten. Dies ist besonders wichtig, wenn es Unternehmen an spezifischem Fachwissen mangelt oder sie mit schwerwiegenden Vorfällen wie groß angelegten Angriffen konfrontiert sind, bei denen Partnerschaften mit ISPs helfen können, Bedrohungen wie DDoS-Angriffe abzuschwächen.

Die Bildung von Reaktionsteams erfordert die Beantwortung von Schlüsselfragen, um das Team auf die individuellen Bedürfnisse des Unternehmens zuzuschneiden:

- Funktioniert das Team am besten als zentralisiertes Modell oder verteilt auf mehrere Standorte?
- Wer koordiniert die Arbeit der internen und externen Teams, einschließlich Einrichtungen wie US-CERT?
- Wie wirken sich die Branchenvorschriften auf die Art(en) der Unterstützung bei Zwischenfällen aus, die das Unternehmen entwickeln oder mit denen es zusammenarbeiten kann?
- Gibt es genügend internes Personal für eine zeitnahe Störungsverwaltung, oder ist eine teilweise/vollständige Auslagerung erforderlich?
- Wie hoch sind die Anforderungen an die Verfügbarkeit des Notfallteams unter Berücksichtigung der 24x7x365-Rufbereitschaft und des Vollzeit- bzw. Teilzeitsupports?
- Welche Budgetüberlegungen sind notwendig, um das Team zu finanzieren und Gehälter, PTO, Qualifikationsdefizite und Weiterbildung abzudecken?
- Welche Optionen gibt es für kleinere Organisationen, um Vermögenswerte zu schützen, wenn spezielle Teams nicht möglich sind, und welche Planung ist erforderlich, um im Bedarfsfall schnell reagieren zu können?

Diese Informationen sind von unschätzbarem Wert für Entscheidungen über die Art der erforderlichen Sicherheitsvorrichtungen, einschließlich der Beschaffung von Dienstleistungen zur Gewährleistung eines umfassenden Schutzes. Nicht alle Lösungen erfüllen die gleichen Funktionen. Warum also sollte eine generische Lösung für solch dynamische Technologien die richtige sein? **Die Antwort ist, dass, wie im Fall von Apple Produkten, generische Lösungen oft nicht die beste Lösung sind, da sie nicht die umfassende Abdeckung und den Einblick bieten, den speziell entwickelte Produkte wie Jamf Protect - unsere speziell entwickelte Apple Endpoint-Sicherheitslösung - bieten.**

II: Aufdeckung und Meldung

Identifizieren von Bedrohungen

> „Wenn man nur einen Hammer hat, sieht alles wie ein Nagel aus.“
>
> **- Benjamin Franklin**

Dieses Zitat bezieht sich auf das **Gesetz des Instruments**, eine kognitive Voreingenommenheit, die ein übermäßiges Vertrauen auf ein vertrautes Instrument beinhaltet und dazu führen kann, dass man nur einen Teil des Bildes sieht. Betrachtet man das Verhältnis zur Sicherheitslage der Geräte in Ihrem Unternehmen ausschließlich durch die InfoSec-Brille, so ist die Sicht versperrt, was zu einem ernsten Problem wird, wenn kritische Informationen über den Zustand Ihrer Geräte nicht sichtbar sind. Dieser fehlende Einblick in den Gerätezustand verkompliziert die Situation noch weiter und kann zu noch größeren Auswirkungen führen und sich negativ auf die Sicherheitslage des Unternehmens auswirken, weil eine Bedrohung oder Schwachstelle nicht sichtbar war.

Sichtbarkeit ist der Schlüssel zu angemessenen Reaktionen. Und das sind die beiden Schlüsselphasen, in denen die richtigen Werkzeuge - in Verbindung mit aktuellen Daten - den Unterschied zwischen der schnellen Lösung eines Problems und dem Ausbleiben einer Lösung ausmachen können und werden:

1. Bevor der Alarm ausgelöst wird

2. Während der Sanierungsphase selbst

Warnungen und Benachrichtigungen

Bevor Sie eine Meldung erhalten, muss diese ausgelöst werden. Idealerweise sollten die Tools des Unternehmens Warnfunktionen bieten, indem sie die Endpoints mit verschiedenen Methoden aktiv überwachen und sich nicht nur auf signaturbasierte Ansätze für bekannte Malware verlassen. Darüber hinaus kann ein robuster Prozess, der Heuristiken oder Analysen verwendet, potenzielle Malware und andere Bedrohungen erkennen, einschließlich riskanter Aktionen oder ungewöhnlichem Mitarbeiterverhalten auf der Grundlage von Mustern.

Verhaltensanalysen sind nützlich, um Teams vor potenziellen Bedrohungen durch unbekannte Malware-Varianten zu warnen, für die möglicherweise keine Erkennungsdefinition verfügbar ist. Dieses System ermöglicht es der IT-Abteilung, Indikatoren zu priorisieren, sobald eine Anomalie entdeckt wird. Während der Untersuchung müssen die Teammitglieder die Genauigkeit der Entdeckungen bestätigen, um falsche oder echte positive Ergebnisse zu erkennen. Die Bestätigung von Fehlalarmen spart Zeit und Unternehmensressourcen, während die Überprüfung von echten Fehlalarmen die Entsendung geeigneter Ressourcen ermöglicht, um zu verhindern, dass sich Bedrohungen ausbreiten und größere Auswirkungen oder potenzielle Datenverletzungen verursachen.

Streaming von Protokollierungsdaten an SIEM

Diese Protokolle dienen nicht nur der Anzeige oder Fehlerbehebung von App-Abstürzen, sondern liefern auch wertvolle Informationen über System- und App-Prozesse. Während es bei einem Cybersecurity-Vorfall kontraproduktiv erscheinen mag, in einem Meer von Protokollen zu wühlen, liegt der Schlüssel in der Zentralisierung, Organisation und Analyse spezifischer sicherheitsrelevanter Daten, die wichtige Erkenntnisse in den Vordergrund rücken.

Angefangen bei der Protokollerfassung kann die schiere Anzahl der Geräte in einem Unternehmen überwältigend sein. Wenn dann noch der Zugriff auf Protokolle von verteilten Arbeitsplätzen hinzukommt, wird die Aufgabe noch schwieriger. Das manuelle Sortieren und Analysieren relevanter Daten aus Protokollen kann Stunden dauern oder große Teams beschäftigen.

Hier kommt SIEM (Security Information and Event Management) ins Spiel. SIEM spielt eine entscheidende Rolle in den Sicherheitsprozessen Ihres Unternehmens, indem es:

- Aktuelle Sicherheitsbedrohungen identifiziert, die Endpoints betreffen.
- Teams bei der raschen Reaktion auf Vorfälle unterstützt und deren Einstufung, damit Ihre Teams Sicherheitsvorfälle beheben und lösen können.
- Überprüfung und Gewährleistung der Einhaltung von Normen und Vorschriften.

SIEM analysiert schnell Protokolle von allen Endpoints und bietet Einblicke in den betrieblichen, funktionalen, technischen und Sicherheitsstatus von Apps und Daten auf dem Endpoint. Sie beantwortet Fragen wie die folgenden:

- Was sind die Patch-Stufen eines Geräts?
- Welche Aktionen wurden vom System durchgeführt?
- Wann wurden die Prozesse ausgeführt?
- Von wo aus hat das Gerät kommuniziert?
- Warum hat sich das Gerät, die App oder der Thread auf eine bestimmte Weise verhalten?
- Wer hat eine bestimmte Aufgabe oder Aktion durchgeführt?
- Wie wurde diese Sicherheitslücke ausgenutzt?

III. Triage und Analyse

Analysieren Sie Bedrohungen

Bevor man einfach auf jede erkannte potenzielle Bedrohung reagiert, ist es wichtig, die Möglichkeit von Fehlalarmen oder Fehldiagnosen zu prüfen.

Der zentrale Zweck von Triage und Analyse ist:

- Untersuchen Sie das festgestellte oder gemeldete Problem
- Priorisierung von Sicherheitsereignissen nach Schweregrad
- Zuweisung der für die Analyse der Daten erforderlichen Ressourcen
- Feststellung der Gültigkeit einer Bedrohung oder eines Angriffs

Rationalisierung der Analyse mit SIEM

Ihre SIEM-Lösung sammelt Protokolldaten, sodass Ihre IT- und Sicherheitsteams diese nutzen können, um sortierte Daten genau zu analysieren, bevor sie präzise Maßnahmen ergreifen, um Bedrohungen zu entschärfen und Probleme mit minimalem Ressourcenaufwand zu beheben. Oder noch besser: Sie **erweitern die SIEM-Funktionalität** durch die Integration mit ihren MDM- und/oder Endpoint -Sicherheitslösungen, um **kritische Datensicherheitspunkte zu visualisieren** und automatisierte Abhilfeworkflows in dem Moment auszuführen, in dem Bedrohungen identifiziert werden, um noch schneller auf Vorfälle reagieren und sie bereinigen zu können.

Vorbeugung gegen bekannte Bedrohungen

Die Reaktion auf Vorfälle zielt darauf ab, erkannte Bedrohungen zu bekämpfen, aber die proaktive Vorbeugung bekannter Bedrohungen ist wichtiger als die Reaktion auf einen Angriff. Ein umfassender Plan zur Reaktion auf Vorfälle beinhaltet verschiedene Tools und Funktionen, um Cybersecurity-Probleme aus mehreren Perspektiven zu verhindern. Eine Defense-in-Depth-Strategie, die Sie darauf vorbereitet, Bedrohungen durch verschiedene Verteidigungsschichten abzufangen, bevor Sie ihnen zum Opfer fallen, verlässt sich nicht auf einen einzigen Ansatz.

Eine wichtige Verteidigungsebene ist die Analytik, die sich am **MITRE ATT&CK-Framework** orientiert , einer Sammlung von realen Taktiken und Techniken des Gegners. Diese globale Wissensbasis fördert die Zusammenarbeit zwischen Unternehmen, Entwickler*innen, InfoSec-Fachleuten und der Sicherheitsgemeinschaft, um Cybersicherheitspraktiken zu verbessern, Risiken zu minimieren und die Bedrohungsabwehr zu maximieren.

Die Integration dieser Funktion in Ihre Endpoint-Sicherheitslösung schützt Geräte, die auf Unternehmensressourcen zugreifen, vor den Risiken, die von bekannten Bedrohungen und deren Angriffsvektoren ausgehen. MITRE ATT&CK **ordnet jede Bedrohung einer Analysefunktion innerhalb Ihrer Endpoint-Sicherheitslösung** zu und ergreift Maßnahmen, um Bedrohungen während der aktiven Überwachung zu blockieren oder unter Quarantäne zu stellen.

Diese Analysen decken Desktop-Betriebssysteme ab und befassen sich mit modernen Bedrohungen, einschließlich solcher, die auf mobile Geräte für den Unternehmens- und Privatgebrauch abzielen. Dieser ganzheitliche Ansatz umfasst neben der Sicherheit von Desktop-Betriebssystemen auch die Abwehr von Bedrohungen für mobile Endgeräte (MTD). Bei komplexen Bedrohungen oder solchen, die mit anderen konvergieren, um sich der Erkennung zu entziehen, arbeitet die Analytik mit Geräteverwaltungslösungen für fortschrittliche SOAR-ähnliche Workflows (Security Orchestration, Automation and Response) zusammen. In Situationen, in denen ein Eingreifen erforderlich ist, steuern Daten und Analysen die Reaktion des Reaktionsteams, z. B. die Einschränkung der Netzwerkkonnektivität, die Eindämmung der Infektion auf den betroffenen Endpoint und die Verhinderung der Ausbreitung von Bedrohungen im gesamten Unternehmensnetzwerk.

Jagd auf unbekannte Bedrohungen

Die Integration der SIEM-Technologie in die Endpoint-Sicherheit bietet Sicherheitsteams erweiterte Funktionen für die Analyse der Bedrohungslage. Wenn Sie die umfangreichen Telemetriedaten von Endpunktsicherheitsprodukten und einem SIEM mit dem Fachwissen Ihres Sicherheitsteams kombinieren, können Forscher die Systemprozesse genauer unter die Lupe nehmen und die neuesten Telemetrie- und Protokolldaten in einer Konsole nutzen, um potenzielle unbekannte Bedrohungen aufzuspüren, zu identifizieren und zu beseitigen.

Spezielle Teams für die Bedrohungsjagd, wie **Jamf Threat Labs (JTL)**, untersuchen und aktualisieren die Sicherheitsregeln für Endpoints kontinuierlich, um die Endpoints vor den neuesten Bedrohungen zu schützen. Wenn Ihr Unternehmen nicht über ein Team zur Bedrohungsjagd verfügt, insbesondere bei mittleren und größeren Unternehmen, empfiehlt es sich, ein Produkt zu wählen, das bereits umfangreiche Ressourcen zur Bedrohungsjagd bereitstellt, um die Endpoint-Sicherheit auf dem neuesten Stand zu halten, da sich die Taktiken der Bedrohungsakteur*innen schnell ändern und neue, unbekannte Bedrohungen auftauchen.

Kleinere Unternehmen, die nicht über die Ressourcen für ein internes Team verfügen, sollten sich mit Dienstleistern zusammenschließen, um ein Team zur Bedrohungsjagd aufzubauen. Diese Zusammenarbeit hilft bei der proaktiven Identifizierung potenzieller Bedrohungen, die möglicherweise unbemerkt geblieben sind oder im Allgemeinen nicht bekannt sind, und schützt das Unternehmen vor dem Abgreifen von Daten, die sich der Entdeckung entziehen.

IV. Eingrenzung und Neutralisierung

Reaktion und Abhilfemaßnahmen

Der Prozess der Reaktion auf Vorfälle umfasst Überwachung, Erkennung, Untersuchung und Behebung. Die Behebung von Problemen, die als solche identifiziert wurden, erfolgt mit anderen Mitteln, um die Probleme zu beheben und die betroffenen Geräte wieder in den Normalzustand zu versetzen. Die Effektivität der Reaktion auf Vorfälle und der Abhilfemaßnahmen hängt von unternehmensspezifischen Faktoren ab, wie z. B. Risikofaktoren, Fähigkeiten, Sicherheitstools, Partnerschaften, Richtlinien, Vorschriften, Sicherheitspläne und Budget.

Endpoint-Verwaltungs-Tools sollten eine solide Unterstützung für die von ihnen verwalteten Geräte bieten. In einer Applezentrierten Umgebung kann fehlende Unterstützung für die neuesten Apple Sicherheits- und Geräteverwaltungs-Frameworks die Fähigkeit des Unternehmens beeinträchtigen, schnell auf Bedrohungen zu reagieren. Umfassender Support steht im Einklang mit den IT-/Sicherheitsrichtlinien des Unternehmens und verringert die Belastung der Teams bei Zwischenfällen oder Change-Verwatlungs-Projekten.

Die richtigen Instrumente sind entscheidend, denn Verzögerungen, unzureichende Berichterstattung oder ineffiziente Abhilfemaßnahmen können kostspielige Folgen haben. Eine nahtlose Integration, die im Hintergrund arbeitet, um Geräte zu schützen und Probleme schnell zu beheben, beruht auf Prozessen, die harmonisch mit speziell entwickelten Technologien zusammenarbeiten, wie beispielsweise Jamf Lösungen für die Apple Infrastruktur. Diese Lösungen gewährleisten Sicherheit, optimale Leistung, Commpliance und sofortigen Support mit den neuesten Funktionen.

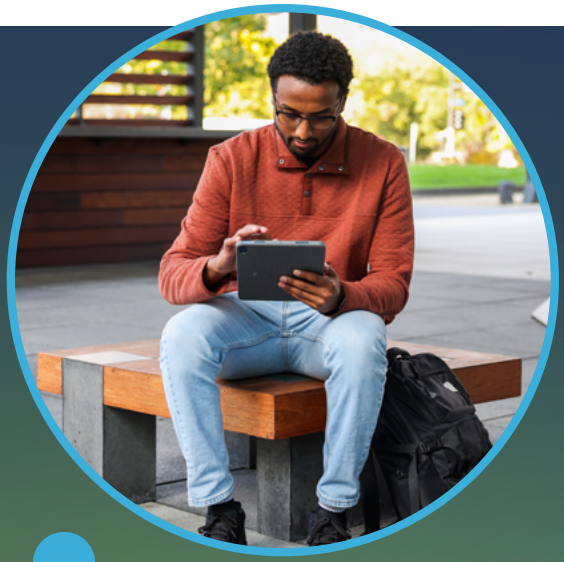
Erweiterte Workflows zur weiteren Absicherung Ihrer Umgebung und zur Unterstützung bei der Reaktion auf Vorfälle und deren Behebung.

Bereitstellung von Geräten

Die Bereitstellung neuer Geräte für die Benutzer*innen oder der Zugriff auf die persönlichen Geräte der Benutzer*innen, die für die Arbeit verwendet werden, birgt eine zusätzliche Risikodimension. Haben die Benutzer*innen ihre persönlichen Geräte richtig konfiguriert? Wie kann die IT-Abteilung überprüfen, ob die Sicherheitslösungen auf den Endpoints aktiviert sind? Was kann getan werden, um das Risiko auf kompromittierten Geräten zu begrenzen?

Die Antworten auf diese Fragen werden durch Bereitstellungsworkflows gegeben, die an zentral verwaltete Zugangsdaten als Teil einer **Identity and access management (IAM)** gebunden sind: eine Lösung, die von der ersten Bereitstellung des Geräts über den gesamten Lebenszyklus des Geräts reicht. Durch den Einsatz von IAM sind die Zugriffsberechtigungen an die Anmeldeinformationen des Benutzers/der Benutzerin gebunden, sodass nur die erforderlichen Berechtigungen für die Ressourcen erteilt werden und der Zugriff bei Bedarf just-in-time erfolgt.

Darüber hinaus bietet die Bereitstellung durch Zero-Touch-Bereitstellungs-Workflows eine grundlegende Unterstützung für Aufgaben zur Reaktion auf Vorfälle und Abhilfemaßnahmen. So wird nicht nur **sichergestellt, dass die Endpoints von Anfang an korrekt eingerichtet sind** , sondern auch, dass im Falle eines Vorfalls zusätzliche Schutzmaßnahmen ergriffen werden können, um die Risiken von Bedrohungen zu mindern und gleichzeitig die Auswirkungen von Angriffen zu minimieren, um die Wiederherstellungsprozesse zu beschleunigen.



Identity und Zugang

Identity and access management (IAM) geht über Konten und Passwörter hinaus, um den Austausch sensibler Daten zu sichern. Es hat sich zu einer eigenen **umfassenden identitätsbasierten Sicherheitslösung entwickelt**, die Ressourcen durch mehrere Arbeitsabläufe effektiv vor der modernen Bedrohungslandschaft schützt, die über die bloße sichere Verbindung von Benutzern zu Unternehmensressourcen oder die Anforderung, ein starkes Passwort festzulegen, hinausgeht.

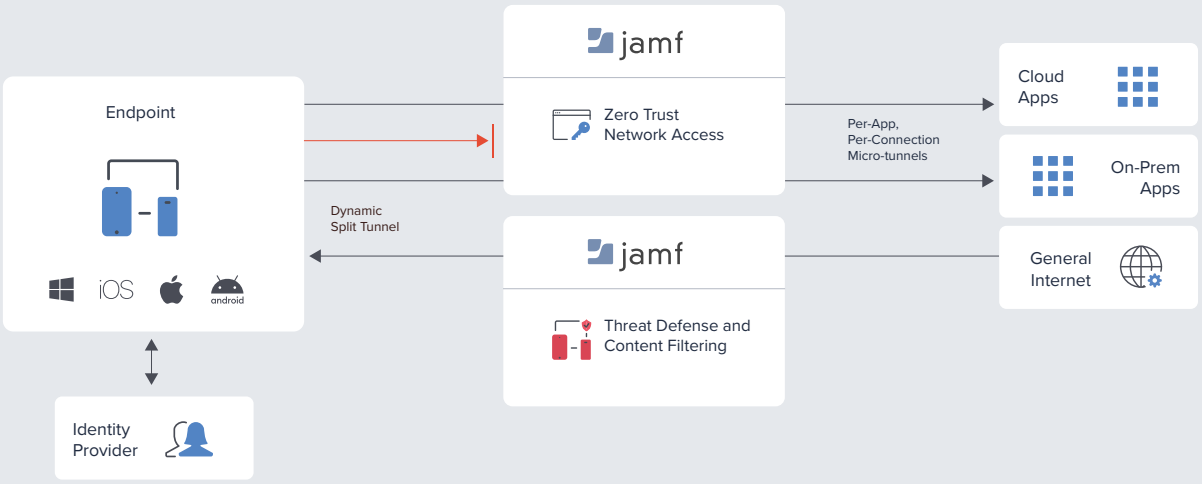
Durchsetzung der Politik

Die richtlinienbasierte Verwaltung ist von entscheidender Bedeutung für die Aufrechterhaltung der Sicherheitslage eines Geräts gemäß einer akzeptierten Basislinie. Verschiedene Faktoren wirken sich auf die Sicherheitslage aus, z. B:

- App-Updates
- Neue OS-Versionen
- Sicherheitspatches
- Sich entwickelnde organisatorische Anforderungen
- Benutzerverhalten
- Aufkommende Bedrohungen

Richtlinien, die Mindestregelsätze darstellen, helfen dabei, trotz der Unvorhersehbarkeit dieser Faktoren ein bekanntes Sicherheitsniveau aufrechtzuerhalten.

Die Zero Trust Network Access (ZTNA)-Technologie verwendet einen richtlinienbasierten Durchsetzungsrahmen. Geräte und Benutzer*innen werden einer Risikobewertung unterzogen, wenn sie den Zugang zu einer geschützten Ressource beantragen. Bei einem Zero-Trust-Ansatz wird der Zugriff zunächst verweigert und muss dann auf der Grundlage organisatorischer Kriterien gewährt werden. Der Zugang bleibt verweigert, wenn ein Gerät oder ein Benutzer/eine Benutzerin diese Kriterien nicht erfüllt



Sichere Netzwerkverbindungen

Um modernen Bedrohungen wirksam begegnen zu können, brauchen wir moderne Technologien. VPN, eine alte Technologie, die seit Jahrzehnten Netzwerkverbindungen durch Verschlüsselung und Benutzeranmeldeinformationen schützt, wird den Anforderungen heutiger Computerumgebungen und der veränderten Bedrohungslandschaft nicht mehr gerecht. Bei VPN fehlt es an Skalierbarkeit, an der Einhaltung des Prinzips der geringsten Privilegien, an kompensierenden Kontrollen für Angriffe von der Seite, an einer Risikobewertung auf der Grundlage des Geräte- und Benutzerzustands und an der Integration mit zentralisierten Identitätslösungen.

Im Gegensatz dazu sichert ZTNA die Netzwerkverbindungen wie herkömmliche VPN-Lösungen, jedoch ohne deren Nachteile. ZTNA wurde entwickelt, um Sicherheits-Workflows zu bieten, die sich in moderne Lösungen integrieren lassen und die Kompatibilität mit verschiedenen Gerätetypen in der gesamten Infrastruktur gewährleisten. Damit entfallen die administrativen Herausforderungen, die mit der Verwaltung komplexer Konfigurationen verbunden sind, und die finanzielle Belastung durch die Verwaltung älterer VPN-Hardware.

Geräteverwaltung

Mobile Device Management (Mobilgeräteverwaltung, MDM) ist mehr als ein „Nice to have“, wenn es darum geht, sicherheitsrelevante Probleme anzugehen. Von einem einzelnen Endpoint bis hin zur Skalierung Ihrer gesamten Flotte ist dies eine Voraussetzung für die Aufrechterhaltung der allgemeinen Sicherheitslage Ihres Unternehmens. Sie spielt eine entscheidende Rolle, da sie direkt in das Gefüge eines ganzheitlichen Ansatzes zum Schutz von Geräten vor Bedrohungen eingewoben ist. Ähnlich verhält es sich mit Lösungen für die Endpoint-Sicherheit, die mit der Geräteverwaltung verbunden sind. Man kann weder gründlich überprüfen, ob etwas sicher ist, wenn es nicht verwaltet wird, noch kann etwas vollständig verwaltet werden, wenn es nicht sicher ist.

Beispiele für Verwaltungsfunktionen, die die Sicherheit Ihrer Umgebung erhöhen und gleichzeitig die Reaktion auf Vorfälle und deren Behebung unterstützen, sind:

Bestand

Das Führen eines aktuellen Gerätebestands ist unter verschiedenen Aspekten von entscheidender Bedeutung, z. B. für die Verfolgung des Gerätestatus, die Ermittlung potenzieller Risikofaktoren und die Sicherstellung, dass die richtigen Mitarbeiter*innen die richtigen Werkzeuge für ihre Aufgaben haben. Die Bestandsverwaltung geht über die Nachverfolgung von Geräten hinaus und ist der Schlüssel, um sicherzustellen, dass Benutzer*innen, ihre Geräte und Unternehmensdaten jederzeit zugänglich und unter Kontrolle sind.

Ein ausgereiftes IT Asset Management (ITAM)-Programm liefert wertvolle Erkenntnisse für den ganzheitlichen

Sicherheitsplan Ihres Unternehmens:

1. Kritische Geräteinformationen

- Hardware-Details: Gerätetypen, Modelle und Seriennummern
- Software-Informationen: Betriebssystemversion, installierte Apps und deren Versionen
- Sicherheitskonfigurationen: verwaltete Einstellungen, Härtungsprofile und Verschlüsselungsstatus
- Verwaltungsdetails: Anmeldemethoden, Garantieinformationen und verwaltete/überwachte Zustände

2. Grundlage für die Risikobewertung

- Ermöglicht Risikobewertungs- und -quantifizierungsprozesse, die als Grundlage für die Entwicklung umfassender Sicherheitsstrategien dienen.

3. Verwertbare Daten

- Wandelt Bestandsdaten in verwertbare Erkenntnisse um und leitet die nächsten Schritte und iterativen IT-bezogenen Aufgaben an.

4. Unterstützung für Sicherheitsteams

- Stellt den Sicherheitsteams aktuelle Geräteinformationen zur Verfügung und unterstützt in Kombination mit den Basisdaten die Einordnung von Vorfällen, die Reaktion darauf und effiziente Abhilfeworkflows.

Automatisierung

Die Automatisierung von Prozessen ist mehr als nur der Einsatz von Technologie, um die Arbeit des Administrators/der Administratorin zu erleichtern. Sicher, die Möglichkeit, die Bereitstellung von verwalteten Anwendungen, sicheren Konfigurationsprofilen oder die Patch-Verwaltung zu vereinfachen, entlastet die IT-Abteilung bei einigen der üblichen Verwaltungsaufgaben, die sie regelmäßig und massenhaft ausführt.

Der Hauptvorteil der Automatisierung besteht jedoch darin, dass sie die Wahrscheinlichkeit minimiert, dass menschliche Fehler unbeabsichtigte Auswirkungen haben, die andernfalls die Wirksamkeit Ihres Sicherheitsplans beeinträchtigen könnten.

Einige der Möglichkeiten, wie die Automatisierung eine Sicherheitslage verbessern - oder zerstören - kann, sind:

Pause	machen
App-Installer verteilen und aktualisieren Apps und stellen sicher, dass immer die neueste Version installiert ist, um Schwachstellen zu minimieren.	Es sind verschiedene Versionen von Apps installiert, einige aktualisiert, andere nicht.
Konfigurationsprofile werden über Ihre MDM-Lösung verwaltet, eingeteilt und bereitgestellt - eine Interaktion mit dem Benutzer*innen ist nicht erforderlich.	Die Administrator*innen sind darauf angewiesen, dass die Endbenutzer*innen geeignete Gerätekonfigurationen festlegen.
Ein standardisierter Arbeitsablauf konfiguriert die Verschlüsselung und ermöglicht die Verschlüsselung und einen sicher verwahrten Wiederherstellungsschlüssel.	Zum Schutz der Daten wird die Verschlüsselung der Datenträger empfohlen.
Die Garantiedaten werden ab dem Kaufdatum erfasst und nachverfolgt.	Ein beschädigtes Gerät erfordert einen Serviceanruf beim Hersteller zur Reparaturunterstützung.
Die Zero-Touch-Bereitstellung stellt sicher, dass unternehmenseigene Geräte von dem Moment an verwaltungs- und einsatzbereit sind, in dem das Gerät eingeschaltet wird.	Die Benutzer*innen sind dafür verantwortlich, unternehmenseigene Geräte im MDM des Unternehmens zu registrieren.
Unternehmen können fehlende Geräte aufspüren, sie mit MDM-Befehlen sperren und aus der Ferne löschen und sicherstellen, dass die Daten sicher bleiben.	Im Falle von Verlust oder Diebstahl sind die Nutzer*innen dafür verantwortlich, die Daten vor unbefugtem Zugriff zu schützen.
Richtlinienbasierte Workflows führen Updates entsprechend den organisatorischen Anforderungen aus, um das Risiko eines anfälligen, veralteten Betriebssystems zu minimieren.	Die Nutzer*innen sind dafür verantwortlich, das Betriebssystem auf dem neuesten Stand zu halten.

Stellen Sie sich das folgende reale Szenario vor: Das persönliche Gerät eines Benutzers/einer Benutzerin verwendet ein veraltetes Betriebssystem. Sie haben sich dafür entschieden, die Aktualisierung auf das neueste Betriebssystem so lange wie möglich hinauszuzögern, weil sie täglich auf eine App angewiesen sind, die vom neuesten Betriebssystem noch nicht unterstützt wird. Trotz der bekannten Sicherheitsrisiken verwenden sie das anfällige Gerät weiterhin für ihre Arbeit und für private Zwecke.

Wie können Sie die Eindämmung dieser Sicherheitsbedrohung automatisieren und die Unternehmensdaten schützen?

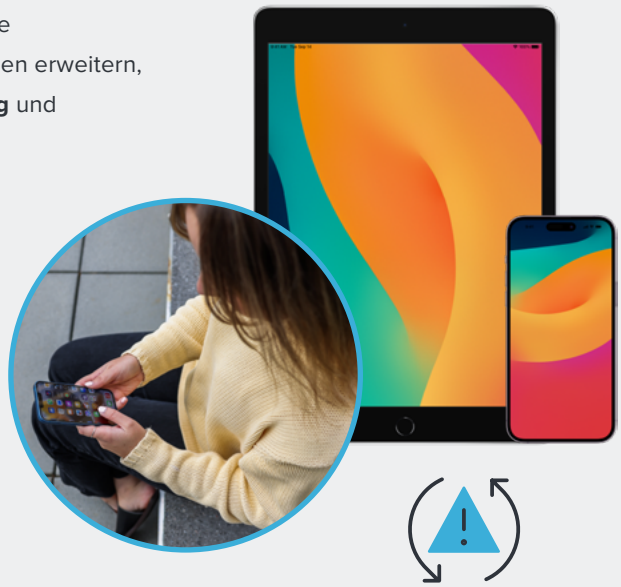
Die Integration Ihrer MDM- und Endpoint Security-Lösungen verbessert die Funktionalität für IT- und Sicherheitsteams und ermöglicht fortschrittliche Workflows zur Reaktion auf Vorfälle und zur Behebung von Problemen.

Die Endpoint-Sicherheitssoftware prüft die Telemetriedaten des persönlichen Geräts anhand von Mindestanforderungen, bevor sie den Zugriff auf sensible Unternehmensressourcen gewährt.

Wenn die erste Anfrage aus Sicherheitsgründen automatisch abgelehnt wird, werden die Telemetriedaten des Geräts sicher mit der MDM-Lösung geteilt. MDM-Richtlinien schreiben vor, dass auf dem Gerät das neueste Betriebssystem ausgeführt werden muss, was eine Aufgabe zur Aktualisierung des Betriebssystems auslöst.

Nach Abschluss der Aufgabe scannt die Endpoint Security-Lösung das Gerät erneut, um die Bedrohungsabwehr zu bestätigen. Im Erfolgsfall wird der Zugang zu den Unternehmensressourcen gewährt, andernfalls bleibt die Anfrage verweigert, und es sind möglicherweise weitere Abhilfemaßnahmen erforderlich.

Die Automatisierung geht über diesen Punkt hinaus. Ähnlich wie die Integrationen mit IAM-Lösungen die Identitäts- und Zugriffsfunktionen erweitern, erweitert die Integration zwischen Ihrer **erstklassigen MDM-Lösung** und verschiedener Software die Funktionalität.



Vertraue nie – überprüfe immer!

Endpoint-Sicherheit

In einem idealen Szenario schützt ein umfassender Endpoint-Schutz alle Apple Computer und mobilen Geräte vor der modernen Bedrohungslandschaft. Allerdings ist das reale Geschäft nicht ausschließlich auf Apple Hardware beschränkt, und Apple best zu sein, bedeutet nicht, dass es nur Apple gibt.

Die meisten Umgebungen sind plattformübergreifend, sodass ein umfassender Endpoint-Schutz die Unterstützung über das Apple Ökosystem hinaus auf Windows- und Android-Endpoints ausdehnen muss, um einen wirksamen Schutz vor neuen und sich weiterentwickelnden Bedrohungen zu gewährleisten. Dieser ganzheitliche Ansatz gewährleistet effiziente Defense-in-Depth-Strategien, die verschiedene Gerätetypen und Betriebssystemarchitekturen abdecken.

Da kein Betriebssystem gegen Bedrohungen immun ist, helfen Sicherheitslösungen mit leistungsstarken und flexiblen Arbeitsabläufen Unternehmen, mit Apple und anderen mobilen Geräten erfolgreich zu sein. Bei diesen Lösungen stehen die Datensicherheit, der Schutz der Privatsphäre der Benutzer*innen und die Produktivität der Endbenutzer*innen im Vordergrund.

Endpoint-Sicherheitsfunktionen, einschließlich mobiler Bedrohungsabwehr und Schwachstellenverwaltung, ermöglichen die Verwaltung und dem Schutz von Geräten während ihres gesamten Lebenszyklus.

Mobile Threat Defense

Die Sicherung von Daten kann eine Herausforderung sein, insbesondere für Unternehmen mit verteilten Mitarbeiter*innen. Die Schwierigkeit wird noch größer, wenn die Integration zwischen Verwaltungs- und Sicherheitstools fehlt und sich die Bedrohungsmethoden weiterentwickeln. Diese Situation macht es InfoSec-Expert*innen schwer, schnell und effizient auf Bedrohungen zu reagieren.

Mobile Bedrohungen tragen zu diesen Herausforderungen bei, da sie eine neue Grenze für Sicherheitsvorfälle darstellen. Bei geschätzten 6,7 Milliarden Smartphone-Nutzer*innen weltweit wird zunehmend auf mobilen Geräten gearbeitet, was natürlich dazu führt, dass Bedrohungsakteur*innen ihre Angriffe auf mobile Endpoints konzentrieren (Statista-Prognose 2023). Zu den mobilen Geräten gehören Smartphones, Laptops, Tablets, Wearables und sogar einige IoT-Geräte, mit denen mehrere Betriebssysteme wie Apple, Windows, Android und Google Chromebooks eingeführt werden.

Mobile Geräte stellen ein erhebliches Risiko dar, was die Notwendigkeit einer umfassenden Sicherheitslösung unterstreicht, die dem Schutz der Unternehmensressourcen Priorität einräumt, indem sie die Sicherheitskontrollen so ausrichtet, dass Bedrohungen durch mobile Geräte ebenso effektiv verhindert werden wie Bedrohungen durch andere Geräte im gesamten Unternehmen.

Verwaltung von Schwachstellen

Laut NIST ist das Common Vulnerabilities and Exposures (CVE)-System eine Liste von Einträgen, die eine Identifikationsnummer, eine Beschreibung und mindestens eine öffentliche Referenz für öffentlich bekannte Sicherheitslücken im Internet enthält. Es hilft dabei, Schwachstellen im Computercode zu identifizieren, zu beschreiben und zu referenzieren.

Um die Schwachstellen von Betriebssystemen oder Apps in Ihrer Umgebung zu ermitteln, ist jedoch häufig eine separate Software zur Bewertung von Schwachstellen erforderlich. Diese Software, die von Pen-Tester*innen verwendet wird, erkennt Bedrohungen und klassifiziert sie anhand von Schweregraden.

Die Verwendung eines eigenständigen Tools zur Schwachstellenbewertung erfordert mehr Ressourcen als die direkte Integration dieser Funktion in Ihre bevorzugte Endpunktsicherheitslösung. Die Integration macht es zu einem wesentlichen Bestandteil der Arbeitsabläufe Ihres InfoSec-Teams bei der Abwehr von Bedrohungen, der Reaktion auf Vorfälle und der Behebung von Problemen, um Risiken zu minimieren und die Compliance zu gewährleisten.

Die Integration der Schwachstellenverwaltung in Jamf Protect verbessert die Reaktion auf Vorfälle, da sich Sicherheitsexpert*innen proaktiv auf Risiken vorbereiten und diese abmildern können. Dieser Ansatz ist proaktiver, als darauf zu warten, dass eine App oder ein Betriebssystem ausgenutzt wird, bevor auf den Vorfall reagiert wird.

Trusted Access

Drei Sicherheitsparadigmen - **eine ganzheitliche Plattform.**

Eine durchgängige, Applezentrierte Lösung, die Geräteverwaltung, Identitätsbereitstellung, sichere Konnektivität und Endpoint-Sicherheit in eine umfassende, ganzheitliche und zentralisierte Plattform integriert.

...sondern eine, die flexibel genug ist, um den netzwerkinternen und mehrschichtigen Sicherheitsschutz zu erweitern und gleichzeitig die Workflows für die Reaktion auf Vorfälle und die Behebung von Problemen für unterstützte Plattformenzu optimieren.

Verwaltung	Identität	Sicherheit
• Halten Sie Endgeräte und Apps mit Patches auf dem neuesten Stand • Optimale Leistung ohne Beeinträchtigung von **Sicherheit** und **Datenschutz** • Automatisierte Beseitigung von Sicherheitsbedrohungen zur Risikominderung • Maximierung des **mehrschichtigen Sicherheitsschutzes**/ Verteidigung in der Tiefe	• Aufrechterhaltung der Compliance durch **kontextabhängige** Richtlinien • Bereitstellung von Cloudbasierten Identitäten und zentrale Verwaltung von Passwörtern • Sichere Verbindungen aus der Ferne mit der **ZTNA-**Technologie der nächsten Generation • Implementierung von **Multifaktor-Authentifizierungs-**Workflows (MFA) für eine zusätzliche Ebene der Zugriffssicherheit	• Überwachen Sie die Verfahren der Systeme und verhindern Sie Bedrohungen durch Malware • Analysieren Sie die Gesundheit der Endpoints regelmäßig, um Verschiebungen der Basislinien zu minimieren. • Gewinnung umfangreicher Telemetriedaten als Entscheidungsgrundlage für IT- und Sicherheitsteams • Fortschrittliches **maschinelles Lernen** (ML) und **eine Threat Intelligence** Engine (MI:RIAM) sorgen für die Suche nach und die **Abwehr von Bedrohungen** - auf dem Gerät und im Netzwerk

Angleichung an die Compliance

Angesichts der ständigen Bedrohungen und neuartigen Angriffe, über die in den Medien berichtet wird und die die IT- und Sicherheitsteams unter Druck setzen, ist die Compliance von entscheidender Bedeutung. In Anbetracht der geltenden Vorschriften ist es eine große Herausforderung, sicherzustellen, dass jedes Gerät, jeder Benutzer/jede Benutzerin oder jedes Datenelement den Vorschriften entspricht.

Ein Beispiel: Mobile Geräte, die am 24. Oktober 2023 um 9:59 Uhr mit iOS 17 ausgestattet waren, wurden eine Minute später technisch nicht mehr konform, als iOS 17.1 verfügbar wurde. Dies verdeutlicht, dass die Compliance subjektiv und vergänglich ist.

Es ist wichtig, die Compliance von den Sicherheitsvorkehrungen zu unterscheiden. Compliance ist ein flüchtiger Zustand, während Sicherheit ein Fahrplan ist, um ihn zu erreichen. Die Überschneidung von Compliance-Anforderungen und Sicherheitskontrollen bildet häufig ein Framework, der IT- und Sicherheitsteams bei der Erfüllung der Compliance-Ziele hilft.

Die Kombination von Lösungen ermöglicht es den Verantwortlichen, die Compliance durch richtlinienbasierte Verwaltungs-Workflows durchzusetzen. Diese Automatisierung stellt sicher, dass Geräte wieder in Übereinstimmung gebracht werden, nachdem sie aus dem Rahmen gefallen sind, ausgelöst durch Warnungen wie fehlende Apps oder Fehlkonfigurationen nach einem Betriebssystem-Update.

V. Aktivitäten nach einem Vorfall

Information über künftige Prozesse und Praktiken

Befunde dokumentieren

Halten Sie alle Befunde fest, unabhängig von ihrer Größe und Bedeutung. Die Dokumentation informiert die Beteiligten über die Ursachen und Lösungen von Problemen. Es fördert die Zusammenarbeit bei der Entwicklung besserer Lösungen und der Optimierung von Vorfallsreaktionen, Abhilfeworkflows und Richtlinien.

Gelernte Lektionen

Die Dokumentation geht über die Aufzeichnung von Ereignissen hinaus; sie liefert wertvolle Erkenntnisse. Die regelmäßige Überprüfung der Ergebnisse verbessert den Prozess der Reaktion auf Vorfälle und deren Behebung. Sie führt zu größerer Effizienz, eliminiert unnötige Schritte und verbessert den Gesamtwert.

Kontinuierliche Überwachung

Betrachten Sie Prozesse als zyklisch, nicht linear. Nach der Implementierung eines Arbeitsablaufs sollten die Ergebnisse den Beteiligten zur Überprüfung vorgelegt werden. Dieser iterative Ansatz ermöglicht die Analyse, den Vergleich mit den Ausgangswerten und die Anpassung an technologische und verfahrenstechnische Veränderungen. Sie zielt darauf ab, Risiken zu verringern, Auswirkungen zu minimieren und die Effizienz erheblich zu verbessern.

Schulungen

Ziel ist es, bessere, rationalisierte Arbeitsabläufe zu schaffen, die den Sicherheitsaufwand optimieren. Dazu gehört, dass die Reaktions- und Abhilfepläne mit den Aufgaben der IT- und Sicherheitsteams abgestimmt werden. Der Schwerpunkt liegt auf der Erfüllung der besonderen Anforderungen von Unternehmen und Benutzer*innen bei gleichzeitiger Minimierung der Ausfallzeiten.

Zusammenfassung

Wenn Sie bereit sind, den nächsten Schritt bei der Erstellung oder Verstärkung Ihres Reaktions- und Abhilfeplans für Zwischenfälle zu tun, kann Jamf Ihnen helfen.

Testen Sie uns kostenlos, um zu sehen, wie das möglich ist, oder wenden Sie sich an Ihren bevorzugten Partner, um loszulegen.