Die Anatomie eines Cyber-Angriffs

In der heutigen global vernetzten Welt haben Cyber-Sicherheitsexperten alle Hände voll zu tun, um Bedrohungen abzuwehren. Während Cyberkriminelle nur eine Schwachstelle finden oder eine Reihe von Anmeldedaten kompromittieren müssen, um sich Zugang zu Unternehmensnetzwerken zu verschaffen, müssen Sie als Sicherheitsexperte immer alles richtig machen ... oder Sie gehen das Risiko ein, dass ein nicht konformes Gerät oder nicht konforme Benutzeranmeldedaten die Tür für eine Datenverletzung öffnen.

Wie Thomas Jefferson sagte: „Wissen ist Macht." In diesem Fall kann diese Macht Bedrohungsakteuren Einblicke in die Schwachstellen der Abwehr eines Unternehmens geben, oder sie ermöglicht es Cybersicherheitsexperten, die Art eines gegen sie gerichteten Cyberangriffs zu verstehen.

Dazu sollten Sie sich einmal jede Phase einer Cyber Kill Chain ansehen und die Anatomie eines solchen Angriffs genau verstehen. Auf diese Weise können Sie Risiken minimieren und gleichzeitig den Schutz verbessern.

In diesem Fachbeitrag werden wir:

- Uns die Cyber Kill Chain ansehen
- Zeigen, wie ein Angriff funktioniert
- Die wichtigsten Verbindungen mit kritischen Schutzmaßnahmen abstimmen
- Aufzeigen, wie wichtig es ist, Sicherheitslücken zu schließen

Nochmal auf alles genau eingehen

Die Angriffe variieren, da die Bedrohungen, die Cyberkriminelle verwenden, von den ausgewählten Zielen und deren Schwachstellen abhängen. Die Einzigartigkeit der Angriffe in Kombination mit den Variablen, die sich auf die Sicherheit eines Endpoints auswirken, macht die Cybersicherheit zu einer Mischung aus Kunst und Wissenschaft.

Trotz der unterschiedlichen Bedrohungen, aus denen ein Angriff besteht, gibt es eine Gemeinsamkeit: die Anatomie eines Angriffs oder die Glieder der Cyber Kill Chain, wie sie von Lockheed Martin entwickelt wurde. Diese Kette besteht aus sieben Phasen, die von der Vorbereitung bis zum Einsatz von bösartigen Tools reichen, um das Ziel zu erreichen. Durch die Analyse jeder Phase können Cybersicherheitsexperten Schwachstellen in ihrem Abwehrsystem identifizieren, die Bedrohungsakteure anvisieren und ausnutzen werden, um Schutzmaßnahmen zu umgehen.

> **„Das ist mein Konzept, Und das ist mein Plan"**
>
> **– Tearsfor Fears**

Bevor Sie lernen, wie Sie die Roadmap eines Angreifers lesen können, möchten wir Ihnen die sieben Phasen der Cyber Kill Chain erläutern:

1. **Aufklärungsarbeit:** Es wird sowohl online als auch offline nach Zielen gesucht.
2. **Beschaffung von Tools:** Die Ergebnisse der Suche werden zur Entwicklung und/oder Beschaffung von Werkzeugen verwendet, die in späteren Phasen eingesetzt werden.
3. **Angriff:** Bösartige Tools werden aktiv gegen Ziele eingesetzt, um sich Zugang zu verschaffen.
4. **Ausnutzung der Schwachstellen:** Sobald man sich Zugang verschafft hat, werden Schwachstellen und andere Sicherheitslücken ausgenutzt, um den Zugang weiter auszudehnen.
5. **Installation:** Die Verbreitung von schädlichem Code bildet die Grundlage für den Erfolg des Angriffs.
6. **Übernahme und Kontrolle:** Vor der letzten Phase des Angriffs wird die Kommunikation mit kompromittierten Geräten hergestellt.
7. **Aktionen zum Erreichen der Ziele:** Nachdem alle Vorbereitungen und grundlegenden Arbeiten abgeschlossen sind, setzen die Bedrohungsakteure Tools ein, mit denen sie ihre Ziele erreichen (Erfassen von persönlichen Informationen, Exfiltrieren von Daten, Ausführen von Ransomware usw.)

Es ist Showtime!

Schauen wir uns die einzelnen Phasen der Cyber Kill Chain einmal genauer an. In diesem Abschnitt verwenden wir die verteilte Malware-as-a-Service-Bedrohung **Atomic Stealer** (AMOS), die auf macOS abzielt, als Beispiel für den Aufbau eines Angriffs und wie er in einem realen Szenario ablaufen könnte.

1. Aufklärungsarbeit

In der Phase der Informationsbeschaffung konzentrieren sich die Bedrohungsakteure ausschließlich auf das Auskundschaften ihres Ziels, um detaillierte Informationen über die Infrastruktur des Opfers, die Netzwerktopographie und die vor- und nachgelagerten Dienstanbieter zu erhalten. Jedes Detail hilft ihnen, ein Profil der Organisation zu erstellen, auf die sie es abgesehen haben. Es ist wichtig zu wissen, dass in dieser Phase passive und aktive Aufklärung stattfindet.

Aktiv

Dies kann ein Hinweis für Unternehmen sein, dass sie von invasiven Tools überwacht werden, die digitale Fingerabdrücke hinterlassen, z. B. übermäßig viele fehlgeschlagene Anmeldeversuche oder Netzwerk-Fingerprinting.

Passiv

Dies stützt sich weitgehend auf Open-Source-Aufklärung, um anonym Informationen zu sammeln, ohne dass das Ziel etwas davon mitbekommt. Beispiele hierfür sind:

- Nutzung sozialer Medien, um sich mit Opfern in Branchen mit hoher Wertschöpfung, wie Krypto, zu vernetzen
- Nutzung sozialer Medien, um Mitarbeiter*innen in wichtigen Funktionen innerhalb des Zielunternehmens kennenzulernen
- Identifizierung von Partnerschaften mit Anbietern, um Dienstleistungen zu ermitteln, die von der Zielorganisation zur Abwicklung von Geschäften genutzt werden
- Social Engineering, um Mitarbeiter*innen dazu zu bringen, sensible oder vertrauliche Informationen preiszugeben, um die Erfolgschancen des Angriffs zu erhöhen

2. Beschaffung von Tools

Nach Abschluss der Informationsbeschaffung organisieren die Bedrohungsakteure die gesammelten Informationen und beginnen mit der Anpassung der Tools, die in den ersten Phasen des Angriffs verwendet werden. In unserem Beispiel haben die Bedrohungsakteure mehrere Maßnahmen ergriffen, um Atomic Stealer als Waffe einzusetzen. Sie haben die Malware entwickelt und die DMG ad hoc unterzeichnet. Sie haben es sogar geschafft, spezielle Installationsanweisungen für Benutzer*innen bereitzustellen, um die Gatekeeper-Warnungen von Apple zu umgehen. Es wurde eine falsche Website erstellt, um die echte Arc-Browser-Website zu imitieren, auf der die Besucher*innen aufgefordert werden, die kompromittierte Version der Software herunterzuladen.

HINWEIS: In den Phasen 1 und 2 sind die Sicherheitslösungen nicht besonders effektiv, um die Cyber Kill Chain zu stoppen, da es sich bis Phase 3 meist um Annahmen handelt. Man muss sich das so vorstellen: Im Gegensatz zum Minority Report finden in den Phasen 1 und 2 keine Angriffe statt. Bis jetzt gibt es nur Gedanken, Ideen oder Hypothesen im Kopf eines Bedrohungsakteurs. Mit Phase drei beginnt die Internetkriminalität, und wir müssen warten, bis die Bedrohungsakteure versuchen, einen Angriff zu starten, bevor sie gestoppt werden können.

3. Angriff

In dieser Phase setzen die Cyberkriminellen ihre Konzepte und Planung in die Tat um.

SCHRITT 1. Gefälschte Website geht online

SCHRITT 2. Sie wird über gesponserte Werbung statt über die legitime Arc Browser-Website zur Verfügung gestellt

SCHRITT 3. Der oder die Benutzer*in lädt die Software herunter und führt sie aus, wodurch der Endpoint mit der Atomic Stealer-Malware infiziert wird

Aufgrund der Reichweite gesponserter Anzeigen und der Platzierung an der Spitze der Benutzersuche kann der gezielte Angriff von Personen auf ihren Geräten in relativ kurzer Zeit zu einer Vielzahl infizierter Endpoints führen. Dieser spezielle Angriff wird nicht durch den direkten Besuch der Website gestartet. Die Website dient eher dazu, dass der Angriff unentdeckt bleibt. Wie Jamf Threat Labs feststellte, verbreiten sich Angriffe, die Varianten von Atomic Stealer nutzen, schnell, da die Bedrohungsakteure Phishing-Kampagnen per E-Mail, SMS und über soziale Medien durchführen, um eine größere Anzahl von Opfern zu erreichen.

Lösungen wie **Jamf Pro** und **Jamf Protect** arbeiten zusammen, um Benutzer*innen vor solchen Bedrohungen zu schützen. Erstere nutzt eine Kombination aus Inhaltsfiltern, um Phishing-URLs zu blockieren, selbst wenn die Benutzer*innen auf den Link klicken. Der Endpoint-Schutz überwacht aktiv den Zustand des Geräts und benachrichtigt die Administrator*innen über Änderungen des Konformitätsstatus, während die Anmeldeprofile der Geräteverwaltung die Datensicherheit erhöhen, indem sie geschäftliche Daten auf einem von persönlichen Daten getrennten, verschlüsselten Volumen speichern, um eine Vermischung zu verhindern. Sollten Geschäftsdaten betroffen sein, können Administrator*innen eine automatische Gerätesäuberung initiieren, einschließlich des Löschens sensibler Daten von betroffenen Geräten, um eine Offenlegung zu verhindern.

4. Ausnutzung der Schwachstellen

Auch wenn die Methoden variieren, *bleiben Ziel und Logik laut den umfangreichen Analysen von Jamf Threat Labs letztlich dieselben.* Mit anderen Worten: Die Anmeldeinformationen des oder der betroffenen Benutzer*in sind kompromittiert worden und die sensiblen Daten wurden gestohlen.

Genau das ist das Ziel von Atomic Stealer: der Diebstahl von Benutzerdaten, nachdem die Benutzer*innen durch einen Trick dazu gebracht wurden, ihre Anmeldedaten als Teil des automatischen Aktualisierungsprozesses einzugeben. Dies ist eigentlich ein AppleScript-Aufruf, der auf dem macOS-eigenen Befehl "osascript" basiert.

Es sei darauf hingewiesen, dass die von dieser Malware im Hintergrund ausgeführten Aktionen zwar von **Jamf Threat Labs** ausführlich dokumentiert wurden (siehe Abschnitt „Aktionen zum Erreichen der Ziele"), dass aber die Erkennung von Varianten, die auf diesem Schadcode basieren, oder sogar von Varianten, die speziell entwickelt wurden, um sich im Laufe der Zeit weiterzuentwickeln, den Bedrohungsakteuren die Möglichkeit bietet, eine beliebige Anzahl von Aktionen auszuführen, ohne dass die Benutzer*innen bemerken, dass sie gehackt wurden. Zum Beispiel das Ausspionieren durch **Bedrohungen, die Apples Transparenz-, Zustimmungs- und Kontrollsystem umgehen.**

Selbst wenn es Bedrohungsakteuren gelingt, die Anmeldeinformationen eines Benutzers während der Phishing-Kampagne zu kompromittieren, verhindert Jamf Trusted Access weitere Angriffe entlang der Cyber Kill Chain, indem es umfangreiche Telemetriedaten in Echtzeit sammelt und die Administrator*innen über Änderungen des Gerätezustands informiert. Darüber hinaus löst es automatisch Abhilfemaßnahmen aus, wie z. B. die Bereitstellung von Updates zur Behebung von Schwachstellen, und verhindert so, dass die Phase „Ausnutzung von Schwachstellen" fortgesetzt wird.

Was die Anmeldedaten selbst betrifft, so verwaltet **Jamf Connect** die Identität und den Zugang, wodurch die betroffenen Konten deaktiviert werden können, bis eine Reaktion auf den Vorfall erfolgen kann. Für eine schnellere **Reaktion auf Vorfälle und eine schnellere Wiederherstellung** bietet die Integration mit Jamf Protect einen **Zero-Trust-Netzwerkzugriff** (ZTNA), um das Risiko automatisch zu minimieren, indem erkannt wird, wenn gestohlene Anmeldeinformationen zur Kompromittierung anderer Apps/Dienste verwendet werden. Es isoliert die Bedrohungen für die betroffenen Dienste, verhindert aber auch Lateral Movement in Ihrer Infrastruktur und die Benutzer*innen können weiterhin mit den nicht betroffenen Diensten produktiv arbeiten. Darüber hinaus finden bei jeder Anfrage fortlaufende Hardware- und Softwareüberprüfungen statt. Diese stellen eine zusätzliche Schutzebene dar, die den Zugriff auf Unternehmensressourcen durch kompromittierte Geräte und Anmeldeinformationen effektiv deaktiviert, bis verifiziert wurde, dass die betroffenen Geräte wiederhergestellt und konform sind.

5. Installation

Die Bedrohungsakteure führen kontinuierlich bösartigen Code aus und verbreiten Malware. Auf diese Weise erhalten sie ihren Zugang zu kompromittierten Systemen aufrecht, während sie zusätzliche Tests durchführen, um ihre Reichweite durch Lateral Movement im gesamten Netzwerk, mit dem die kompromittierten Geräte verbunden sind, zu vergrößern. Dazu setzen sie benutzerdefinierte und systemeigene Tools wie Befehlszeilendienstprogramme und bösartigen Code ein, um sich Hintertüren einzurichten. Da Atomic Stealer direkt mit AMOS zusammenhängt und sein Ziel nur darin besteht, alle Informationen des Benutzers zu stehlen, ohne irgendwelche Spuren im System zu hinterlassen, unternimmt die Malware in dieser Phase nur minimale Schritte. Bei anderen Angriffen werden in dieser Phase normalerweise die Durchführung laufender und künftiger Operationen unter dem Deckmantel der Tarnung geplant.

Es ist von entscheidender Bedeutung, sich in dieser Phase zu schützen. Dazu sollten **Transparenz und Sicherheit genutzt werden, um sicherzustellen, dass die Compliance** eingehalten wird und bekannte Bedrohungen erkannt, verhindert und beseitigt werden. Durch eine aktive Überwachung des Gerätezustands werden Administrator*innen über alle Änderungen in Bezug auf die Sicherheitslage eines Geräts informiert, um entsprechende Maßnahmen für die Reaktion auf einen Vorfall einzuleiten. Jamf Protect verhindert, dass bekannter, bösartiger Code ausgeführt wird, indem es Malware-Bedrohungen unter Quarantäne stellt und entfernt, bevor sie ausgeführt werden können. Bei unbekannten Bedrohungen werden die Geräteprotokolle an eine SIEM-Lösung eines Drittanbieters weitergeleitet, um die **Sicherheitsteams** bei der Erkennung und Beseitigung von Bedrohungen zu unterstützen. Diese halten sich möglicherweise in den Systemen versteckt und sammeln Daten, während die Bedrohungsakteure den richtigen Moment abwarten.

6. Übernahme und Kontrolle (C2)

Das Ziel von Atomic Stealer ist es, erstens Ihre Anmeldeinformationen zu stehlen und zweitens die gestohlenen Passwörter zu verwenden, um Ihre Daten zu stehlen. Je nachdem, welche weiteren Zielen der Bedrohungsakteur verfolgt, bedeutet dies nicht, dass der Angriff hier endet. Da der Schlüsselbund eine zentrale, sichere Speicherung von Anmeldeinformationen bietet, erhalten Angreifer durch das Abgreifen dieser Ressource häufig die Schlüssel zu verschiedenen Funktionen, Software und Diensten. Dies kann sehr hilfreich sein, um:

- Sich besseren Zugang zu datenintensiven Ressourcen zu verschaffen
- Die Angriffe durch Lateral Movement auszuweiten
- Mehr Geld zu verdienen durch Verkauf der Daten und/oder Erpressung der Opfer

Das heißt: Mehr Daten bedeuten mehr lukrative Möglichkeiten.

Deshalb ist die Verhinderung der Kommunikation mit kompromittierten Geräten von entscheidender Bedeutung. ZTNA überwacht Endpoints und blockiert Verbindungen zu bösartigen Diensten wie C2-Servern, wodurch Angreifer von der Kommunikation mit kompromittierten Geräten abgeschnitten werden. Darüber hinaus überwacht ZTNA kontinuierlich den Zustand der Geräte, prüft die Anmeldeinformationen auf Konformität, verhindert den Zugriff auf geschützte Ressourcen durch Geräte und Anmeldeinformationen, die kompromittiert wurden, und schränkt den Zugriff auf nicht konforme Geräte ein. Gleichzeitig arbeitet es mit Jamf Pro zusammen, um automatisch Workflows zur Beseitigung von Schwachstellen und zur Wiederherstellung von kompromittierten Geräten auszuführen.

7. Aktionen zur Erreichung der Ziele

In dieser letzten Phase führen die Angreifer ihre Pläne in vollem Umfang aus, sei es:

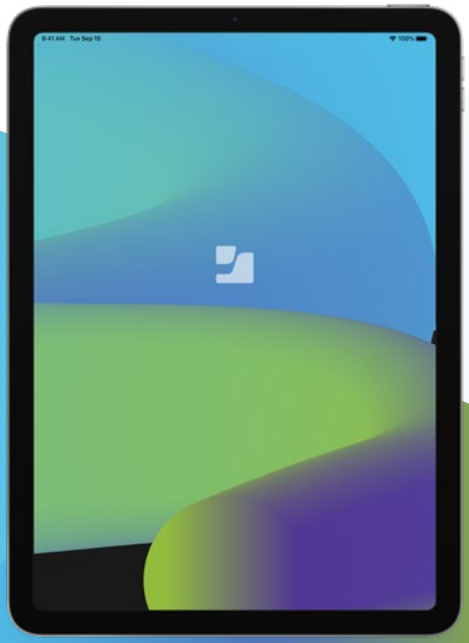
- **Spionage**
- Exfiltration von Daten
- Erpressung
- Angriffe auf die Lieferkette
- Cyber-Terrorismus

Oder eine beliebige Kombination dieser Dinge. Jetzt zeigt sich, ob die Arbeit der Cyberkriminellen Früchte trägt. Dieser Abschnitt lässt sich nur schwer quantifizieren, denn so wie jede Organisation ihre eigenen Bedürfnisse hat, wird auch jeder Angreifer seine Handlungen ganz oder teilweise auf seine eigenen Ziele stützen. Im Fall von Atomic Stealer wird der bereits erwähnte osascript-Befehl verwendet, um das Erscheinungsbild und die Funktionsweise einer legitimen Systemwarnung zu emulieren, aber stattdessen werden die Anmeldeinformationen der Benutzer*innen verwendet, um die verschiedene, vertrauliche Daten aus dem Apple Schlüsselbund zu sammeln:

- Benutzernamen und Passwörter
- Browser-Sitzungscookies
- Sensible Benutzerdaten
- Zahlungskartendaten
- Krypto-Geldbörsen
- System-Metadaten

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

– Chris Triolo, HP



So reparieren Sie die Risse in Ihrer Rüstung

Sicherheitslücken, die durch unzureichende Schutzmaßnahmen und die Konzentration auf Desktop-Betriebssysteme entstehen, machen mobile Geräte unsicher und ermöglichen es Bedrohungsakteuren, durch Kompromittierung in Unternehmensnetzwerke einzudringen.

Mobile Geräte stellen zwar bei weitem nicht das einzige Risiko dar, das zu Datenschutzverletzungen führt, aber es werden kontinuierlich mobile Geräte angegriffen, da diese immer häufiger am Arbeitsplatz eingesetzt werden und private Geräte zunehmend für den Zugriff auf Arbeitsdaten genutzt werden. **Eine Studie von Jamf Threat Labs** hat ergeben, dass „40 % der mobilen Benutzer*innen ein Gerät mit bekannten Schwachstellen verwenden.“ Auf unsicheren Geräten können Bedrohungsakteure aufgrund unkontrollierter Risikofaktoren:

- Bösartigen Code auf Geräten ausführen
- Interne Sicherheitsvorkehrungen umgehen
- Sich Zugang zu nicht autorisierten Geschäftsdaten verschaffen
- Unbefugt an private Daten gelangen
- Benutzer*innen ohne ihr Wissen oder ihre Zustimmung ausspionieren
- Pivot-Angriffe vom infizierten Gerät ausführen, um Netzwerke zu kompromittieren
- Persönliche und geschäftliche Daten sowie Informationen zum Schutz der Privatsphäre exfiltrieren

Apple ist dafür bekannt, dass es Form und Funktion sowie Stil und Substanz miteinander verbindet. Diese Philosophie erstreckt sich auch auf ein Merkmal ihres Designs, das immer mehr an Bedeutung gewinnt: Sicherheit und Datenschutz. In macOS- und iOS-basierten Betriebssystemen sind mehrere Schutzmechanismen integriert, die Geräte, Benutzer*innen und ihre Daten vor unzähligen Bedrohungen schützen – sowohl auf Hardware- als auch auf Softwareebene.

Doch die Bedrohungsakteure entwickeln ihre Angriffe mit neuartigen Bedrohungen und neuen Malware-Varianten immer weiter, wie die wachsende Bedrohung durch Infostealer zeigt. Sicherheit, die allein auf statischen Signaturerkennungs-Engines basiert, reicht nicht mehr aus für den Schutz vor hochentwickelten Bedrohungen. Laut Dark Reading zeigen einige, wie z.B. Atomic Stealer, „völlig unterschiedliche Entwicklungsketten und nicht eine mehr Kernversion, die nur aktualisiert wird.“ Aus diesem Grund **umgehen anspruchsvolle Bedrohungen die integrierten Schutzmechanismen** und gefährden Geräte, Benutzer*innen und Daten.

Ganzheitliche **Integration von Verwaltung, Identität und Sicherheit als eine Lösung.** Sie arbeiten zusammen – sowohl im Netzwerk als auch auf dem Gerät – um bösartigen Datenverkehr umfassend zu blockieren. Außerdem wird verhindert, dass Geschäftsdaten exfiltriert werden. Dadurch sind sie vor Angreifern geschützt. ZTNA unterstützt diesen Workflow, indem es den Zugriff auf geschützte Geschäftsdienste verhindert. Es erkennt automatisch, wenn Anmeldedaten kompromittiert wurden, und deaktiviert diese, um das Risiko zu minimieren. Auch die Telemetriedaten werden sicher und ganzheitlich ausgetauscht. Dadurch können die Workflows automatisch ausgeführt werden, um Risikovektoren zu minimieren, bis die Schwachstellen beseitigt sind. Erst wenn die Endpoints wieder konform sind, wird der Zugang zu den angeforderten Ressourcen genehmigt.

Sicherheitspläne, die auf einem ausgereiften **Defense-in-Depth-Framework** basieren, sind die beste Möglichkeit für Unternehmen, Risiken zu minimieren, bekannte Angriffe zu verhindern und mit automatisierten Problembehebungsmaßnahmen schnell auf Vorfälle zu reagieren, um die Endpoint-Compliance zu gewährleisten.

Durch die Integration und Nutzung mehrerer Lösungen verteidigen sich Unternehmen gegen anspruchsvolle Bedrohungen mit umfassenden Schutzmaßnahmen, um die Risiken auf verschiedenen, ausfallsicheren Ebenen abzufangen und zu minimieren. Gleichzeitig erstrecken sich diese Schutzebenen über das gesamte Unternehmen und bieten eine Basisverteidigung für alle Geräte- und Betriebssystemtypen, die Zugriff auf Unternehmensressourcen und -daten haben.

In einem kürzlich erschienenen **Bericht von Frost Radar: Endpoint Security, 2023** über die Lösungen von Jamf bezeichnete Frost & Sullivan Jamf aufgrund der Defense-in-Depth-Fähigkeiten unserer Lösungen als führend im Bereich Endpoint-Schutz:

- Erkennung von bösartigen Apps, Skripten und Benutzeraktionen in Echtzeit
- Konsistentes Schwachstellenmanagement, Bedrohungsabwehr und Richtlinienüberwachung
- Sicherheitsberichte für alle Mac- und mobilen Plattformen, einschließlich macOS, iOS/iPadOS und Android Zusätzlicher Schutz vor Web-Bedrohungen umfasst diese Plattformen und erstreckt sich auf Windows und Chromebooks.
- Erweitertes Konfigurations- und Auditing-Framework, um Kund*innen bei der Einhaltung komplexer Compliance-Standardszu unterstützen
- Verbesserter Detailgrad der Endpoint-Telemetrie für den Export in Protokollerfassungs- und Analysetools von Drittanbietern
- Konsistente Durchsetzung von Richtlinien und Unterstützung sowohl für unternehmenseigene als auch für private Geräte
- Jmaf Trusted Access ist die einzige Lösung, die speziell für Apple Geräte entwickelt wurde und Geräteverwaltung, Identität und Zugriff und Endpoint-Sicherheit kombiniert.

Schlussfolgerung

Solange Bedrohungsakteure es auf Geräte, Benutzer*innen und Daten abgesehen haben, sind Sicherheitskontrollen erforderlich, um das Risiko zu minimieren und zu verhindern, dass Bedrohungen zu schwerwiegenderen Datenverletzungen führen.

Das Ziel eines kontinuierlichen Sicherheitsplans sollte folgendes beinhalten:

- Bewusstsein für Risiken und Toleranzniveaus
- Implementierung von Kontrollen zur Risikominimierung und Bedrohungsvermeidung auf mehreren Ebenen
- Integration von Lösungen zur Geräteverwaltung, Identität und Zugang sowie Endpoint-Schutz, die zusammenarbeiten
- Zusammenführung von IT- und Sicherheitsteams, um Silos aufzubrechen, die Kommunikation zu fördern und die Reaktion auf Vorfälle zu beschleunigen
- Nutzung von Automatisierungsworkflows, um Bedrohungen schnell zu beseitigen und gleichzeitig benutzerinduzierte Fehler zu minimieren
- Harmonisierung der geschäftlichen Bedürfnisse und Anforderungen mit Standards und Frameworks, um die Sicherheitskontrollen zu verbessern und die Einhaltung der Vorschriften zu gewährleisten
- Zusammenstellen eines „Ersthelferteams“, um schneller auf Vorfälle reagieren zu können. Wenn Sie kein eigenes Team haben, sollten Sie mit einem vertrauenswürdigen Team von Sicherheitsexperten wie Jamf Threat Labs zusammenarbeiten, das Sie bei der Suche nach unbekannten Bedrohungen unterstützt.

Zusammenarbeit mit **Jamf**, einem führenden Unternehmen für die Verwaltung und Sicherheit von Apple-Geräten Nutzung spezieller **Sicherheitsexpertise** wie die Jamf Threat Labs, um Sicherheitslücken zu schließen und gleichzeitig automatisierte Arbeitsabläufe zu implementieren, um Ihre Sicherheitslage gegen hochentwickelte Bedrohungen zu stärken und gleichzeitig sensible Daten zu schützen – für jedes Gerät, das auf geschützte Ressourcen in Ihrer Infrastruktur zugreift. Unabhängig davon, um welches Gerät oder Betriebssystem es sich handelt, wo es sich befindet oder welche Netzwerkverbindung verwendet wird: **Jamf hilft Ihrem Unternehmen, sicher mit Apple zu arbeiten**.