jamf

Sicherheit 360:

Jährlicher Trendbericht 2024

Zusammenfassung

Der jährliche Sicherheitsbericht von Jamf befasst sich eingehend mit der Entwicklung der Bedrohungslandschaft, indem er reale Kundendaten, innovative Bedrohungsforschung und bemerkenswerte Branchenereignisse untersucht. Wir bieten eine durchdachte Bewertung der verschiedenen Angriffsvektoren, die aktiv genutzt werden, um Geräte zu kompromittieren, Benutzer*innen auszutricksen, Organisationen zu infiltrieren und letztendlich wertvolle Geschäftsgeheimnisse und persönliche Daten zu stehlen. Unser Bericht schließt mit einer neuen Perspektive auf branchenübliche Best Practices und umsetzbare Schritte, die Unternehmen jeder Größe unternehmen können, um ihre allgemeine Sicherheitslage zu verbessern.

Einführung

Security 360 bietet eine umfassende Perspektive auf die sich entwickelnde Bedrohungslandschaft. Anhand von realen Daten analysieren wir die wichtigsten Angriffsvektoren des Jahres, bewerten, wie sich Unternehmen an bewährten Sicherheitspraktiken orientieren, und erforschen die Apps, die die Produktivität steigern und Mitarbeiter*innen auf neue Art und Weise miteinander verbinden.

Wir werden unsere Analyse anhand von vier Risikokategorien strukturieren, mit deren effektiver Bewältigung Organisationen auf der ganzen Welt zu kämpfen haben:

I. Geräte-Risiken

II. App-Risiken

III. Malware und Angriffsentwicklung

IV. Webbasierte Risiken

Zusätzlich zu diesen Bedrohungstrends enthält Jamf auch Expertenempfehlungen und Anleitungen, die wir als „Grundlagen“ bezeichnet haben und die Unternehmen dazu auffordern, branchenübliche Best Practices in ihre Geräte-, App- und Infrastrukturverwaltungsprozesse einzubinden.

Einige Beispiele für diese bewährten Verfahren sind die folgenden:

- Die Verwendung von integrierten Verwaltungs- und Sicherheitsprodukten, um die verfügbaren Richtlinienkontrollen zu maximieren und gleichzeitig die Anzahl der Agenten zu minimieren, die Sie pflegen müssen.
- Härtung der Endpoints durch Befolgung der Empfehlungen der Industrie oder regionaler Best Practices
- Schutz vor Bedrohungen durch die Pflege aktueller Betriebssystem- und Appversionen und Patches
- Implementierung mehrschichtiger, tiefgreifender Schutzmaßnahmen

Dieser Bericht soll Unternehmen dabei helfen, sich besser gegen bekannte Bedrohungen zu schützen und gleichzeitig die Angriffsfläche für neue Angriffe zu verringern. Wir werden die fortschreitende Entwicklung des Social Engineering beleuchten und Einblicke geben, wie Sie Ihre Benutzer*innen vor diesen Angriffen schützen können, die verlockender denn je sind.

Abschließend ist es wichtig zu betonen, dass unsere Untersuchungen und Ratschläge für alle Geräte gelten, die mit Geschäftsdaten arbeiten - unabhängig davon, ob es sich um firmeneigene oder BYO-Geräte (Bring your own) handelt - ob Apple, Microsoft oder Android - und von Bedrohungen, die auf alle Plattformen abzielen.

Über den 360-Bericht

Wir wollen die wichtigsten Sicherheitstrends, die den modernen Arbeitsplatz beeinflussen, besser verstehen.

Dazu gehören die Teile des Produktivitätspuzzles - die Geräte, Benutzer*innen und Apps, die alle miteinander verbunden sein müssen, damit die Arbeit erledigt werden kann. Die Informationen zu den wichtigsten Trends, die Statistiken in diesem Papier und wie sie alle zusammenpassen, sind das Ergebnis unserer Analyse von Sicherheitstrends innerhalb unseres Kundenstamms sowie der ursprünglichen Forschung des Jamf Threat Labs Teams zu Betriebssystem- und Appschwachstellen und Studien zu den Tiefen bösartiger und Proof-of-Concept (PoC)-Angriffe, die sich über vier verschiedene Abschnitte verteilen:

Methodik der Forschung

Um die realen Auswirkungen der im diesjährigen Bericht identifizierten Sicherheitstrends zu verstehen und zu quantifizieren, haben wir eine Stichprobe von 15 Millionen durch Jamf geschützten Desktop-Computern, Tablets und Smartphones untersucht.

Unsere Analyse wurde im vierten Quartal 2023 durchgeführt, wobei wir den vorangegangenen 12-Monats-Zeitraum überprüften und weltweit 90 Länder und mehrere Plattformen - insbesondere macOS, iOS/iPad, Android und Windows - abdeckten.

Zum Schutz der Privatsphäre und zur Wahrung höchster Sicherheitsstandards bei der Datenerfassung und -verarbeitung stammen die in unserer Untersuchung analysierten Metadaten aus zusammengefassten Protokollen, die keine personenbezogenen oder organisationsidentifizierenden Informationen enthalten.

Warum das so wichtig ist

Mit dieser Analyse wollen wir keine Ängste schüren, sondern Organisationen und Benutzer*innen über die sich entwickelnden Trends in der Cybersicherheit aufklären, die es derzeit gibt und die sich in Zukunft auf die Sicherheitslage von Geräten und Organisationen auswirken werden. Es informiert Sie auch über die besten verfügbaren Endpoint-Schutzoptionen und wie Sie entsprechende Maßnahmen skalierbar einsetzen können, um alle Aspekte der Geräte-, Benutzer*innen- und Unternehmensdaten zu schützen.

Abschnitt I: Produktrisiken

Mit der Modernisierung der Arbeitscomputer wird die Komplexität der Geräte, die Mitarbeiter*innen täglich nutzen, erheblich gesteigert. Zu dieser Komplexität gehören eingebettete Sensoren zur Erkennung von Kontextinformationen, Co-Prozessoren, die schwere Rechenzyklen auslagern und eine höhere Leistung bieten, sowie mehr Konnektivität von Bluetooth und NFC bis hin zu WiFi und Mobilfunk. All diese Ergänzungen werden im Allgemeinen in bester Absicht vorgenommen. Ein oft übersehener Nebeneffekt ist jedoch, dass jede Komponente die Oberfläche vergrößert, die Angreifende ausnutzen können.

Moderne Geräte sind mit Risiken behaftet. Glücklicherweise können diese Risiken in den meisten Unternehmen mit den richtigen Werkzeugen und Prozessen wirksam verwaltet werden.

Die Aufrechterhaltung eines aktuellen Betriebssystems auf jedem Gerät ist vielleicht die wirkungsvollste Maßnahme, die ein Unternehmen ergreifen kann, aber nicht jeder ist in der Lage, mit dem Innovationstempo Schritt zu halten.

Obwohl es viele Gründe gibt, die Durchführung von Software-Aktualisierungen zu verzögern - von der Angst vor Konflikten bis hin zu übermäßigen Agenten, die nach jeder Aktualisierung auf Kompatibilität getestet werden müssen - bedeutet die Nichtdurchführung von Betriebssystem-Aktualisierungen, dass Arbeitsgeräte wahrscheinlich mit bekannten Schwachstellen betrieben werden, die nur darauf warten, ausgenutzt zu werden.

Diese Schwachstellen betreffen mehr als nur Desktops und Laptops. Wir haben festgestellt, dass **40 % der Mobilfunknutzer*innen ein Gerät mit bekannten Sicherheitslücken verwenden.** Und da immer mehr wichtige Geschäftsapps auf mobilen Geräten ausgeführt werden, sind diese sensiblen Datenspeicher zunehmend Angriffen ausgesetzt, die mit besseren Verfahren wirksamer abgewehrt werden könnten.

Im Jahr 2023 haben wir festgestellt, dass

„8 % der Unternehmen ein mobiles Gerät hatten, das auf einen App Store eines Drittanbieters zugreift.”

„40 % der mobilen Nutzer*innen ein Gerät mit bekannten Sicherheitslücken benutzt haben.”

Im Jahr 2023 haben wir festgestellt, dass „8 % der Unternehmen ein mobiles Gerät haben, das auf einen App-Store eines Drittanbieters zugreift.“ Schwachstellen wie diese, auch wenn die Absicht hinter dem Zugriff auf App-Stores von Drittanbietern harmlos sein mag, sind weit verbreitet mit Apps, die Nutzer*innen oft in die Irre führen, mit dem ausdrücklichen Ziel, die Nutzer*innen zum Herunterladen und Ausführen verdächtiger Apps zu verleiten, deren interne Sicherheit verletzt wurde. Dies könnte möglicherweise führen zu:

Der Ausführung von bösartigem Code auf Geräten
Funktionen wie Gatekeeper und die Sicherheits-API für Unternehmen, die die Ausführung von bösartigem Code verhindern sollen

Der Umgehung interner Sicherheitsvorkehrungen
Warum Sie einschränken wollen, was auf dem Gerät ohne ordnungsgemäße Überprüfung ausgeführt wird.

Der Erlangung von Zugang zu nicht autorisierten Geschäftsdaten
Sensible und vertrauliche Informationen sind nach wie vor eines der Hauptziele von Bedrohungsakteur*innen.

Der unbefugten Beschaffung von privaten Daten
Da es Beweise dafür gibt, dass Apples Transparency, Consent and Controls (TCC) durch unautorisierten Code umgangen wird, ist der Schutz der Privatsphäre für den Schutz von Endpoints von entscheidender Bedeutung.

Dem Ausspionieren von Nutzer*innen ohne ihr Wissen oder ihre Zustimmung
Ähnlich wie beim obigen Punkt nehmen Bedrohungsakteur*innen zunehmend mobile Geräte ins Visier, da diese Geräte immer bei uns sind. Sie nutzen die vernetzte Natur von Mobiltelefonen, um Gespräche abzuhören, SMS abzufangen und Bewegungen über GPS zu verfolgen.

Pivot-Angriffen von infizierten Geräten auf kompromittierte Netzwerke
Dies sind die nächsten Schritte nach der Installation von fehlerhaftem Code.

Konfigurieren Sie für die Compliance

Compliance wird oft als Anpassung an behördliche Richtlinien wie CIS Benchmarks oder NIST-Standards zur Regelung der Datenverarbeitung, -nutzung und -speicherung verstanden. Aber Organisationen haben ihre eigenen Bedürfnisse und Ansätze. Compliance bezieht sich hier auf alle Arten der Gewährleistung, dass Gerätekonfigurationen, Datensicherheit und Benutzer*innen-Workflows standardisiert sind, um sie mit jeder Form von System in Einklang zu bringen und sie vor Bedrohungsakteur*innen zu schützen.

Einige Erkenntnisse zu Trends bei der Einhaltung von Apple spezifischen Sicherheitsfunktionen:

FileVault: Eine grundlegende Funktion, die einen kritischen Schutz der Benutzerdaten durch Verschlüsselung innerhalb des Datenträgers bietet, wurde **„bei 36 % der Geräte im Forschungspool deaktiviert"**, obwohl die Bereitstellung, Konfiguration und Verwaltung von Verschlüsselungsschlüsseln über Ihre MDM-Lösung einfach ist.

Gatekeeper: ...ist mit einer **„Aktivierungsrate von 90 % für den App Store und identifizierte Entwickler*innen"**eine wichtige Sicherheitsebene gegen die Installation von Schadsoftware. Dies ist ein Segen für die Wahrung der Privatsphäre der Nutzer*innen, da Apple jede App überprüft, um sicherzustellen, dass die Datenerfassung das tut, was die Entwickler*innen behaupten.

Firewall: In Anbetracht der Tatsache, dass böswillige Akteur*innen zunehmend mobile Geräte mit webbasierten Bedrohungen ins Visier nehmen, ist es alarmierend, dass die **Firewall-Funktion bei 55 % der Macs deaktiviert ist** Trotz der einfachen Bereitstellung von Konfigurationen über MDM-Lösungen ist die Aktivierung von Firewalls eine bewährte Branchenpraxis, die bekanntermaßen verhindert, dass Geräte eingehende Verbindungen von nicht autorisierten Apps und Diensten akzeptieren.

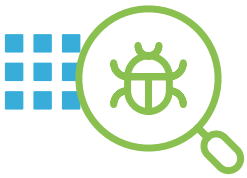
Sperrbildschirm: Eine grundlegende Funktion von Mobilgeräten, die Daten vor unbefugtem Zugriff schützt, aber auch als Entschlüsselungsschlüssel für alle lokal auf dem Datenträger gespeicherten Daten dient. **Im Jahr 2023 hatten „3 % der Geräte die Bildschirmsperre deaktiviert und 25 % der Unternehmen hatten mindestens einen Benutzer/eine Benutzerin mit deaktivierter Bildschirmsperre."**

Abschnitt II: App-Nutzung und wachsende Risiken

Verwaltung von Anwendungsschwachstellen

Sogar ein brandneues Gerät mit der neuesten Hardware und der aktuellsten Betriebssoftware kann anfällig für Angriffe sein, wenn die auf dem Gerät laufenden Apps veraltet sind und Fehler enthalten, die von Angreifer*innen aktiv ausgenutzt werden. Es ist unerlässlich, dass Unternehmen Schwachstellen von der Hardware und der Betriebssystemebene bis hin zu den Apps, die auf dem Gerät laufen, verwalten.

Jamf fand heraus, dass „2,5 % der Geräte im Jahr 2023 eine anfällige App installiert haben." Wenn wir unseren bescheidenen Prozentsatz auf die **geschätzte Zahl von weltweit 16,8 Milliarden mobilen Geräten Ende 2023** hochrechnen, würde dies etwa 420 Millionen gefährdeten Geräten weltweit entsprechen.



2,5 %

der Geräte hatten eine anfällige App installiert

Eine Geschichte von zwei Apps

Bei unserer Untersuchung der Bedrohungslandschaft haben wir zwei grundlegend unterschiedliche Arten von Apps festgestellt, die von Unternehmen genutzt werden. Native (geräteeigene) Apps nutzen Geräteressourcen, um Code auszuführen und den Endnutzer*innen Funktionen bereitzustellen, während Webapps im Internet gehostet werden, in der Regel in SaaS-Umgebungen oder privaten Clouds, und für die Verarbeitung und Datenspeicherung auf Rechenzentren oder Remote-Server angewiesen sind.

Unsere Untersuchungen zeigen, dass Anwendungsrisiken unabhängig von der Art der verwendeten App häufig auftreten:

- Schwachstellen müssen innerhalb der Appsoftware verwaltet werden, und die vernetzte Natur von in der Cloud gehosteten Apps führt dazu, dass sie stärker durch Remote-Manipulationen gefährdet sind als Apps, die auf einem bestimmten Gerät installiert sind.
- In Anbetracht der Tatsache, dass sich zwischen einem Gerät und einer Remote-App wahrscheinlich mehrere Netzwerke befinden, ist der **Schutz von Daten während der Übertragung von größter Bedeutung, wenn es darum geht, die Risiken im Zusammenhang** mit in der Cloud gehosteten Apps zu verwalten.
- **Der Schutz von Daten im Ruhezustand** ist für beide App-Arten gleichermaßen wichtig. Auch wenn in der Cloud gehostete Apps häufig durch die Grenzen des Rechenzentrums geschützt sind, basieren moderne Apps häufig auf Open-Source-Software, gemeinsamen Substraten und gemeinsam genutzten Rechenressourcen.

Unternehmen mit verwalteten Geräten erhalten durch ständige Überwachung einen Einblick in diese Endpoints, aber was ist mit nicht verwalteten Geräten, wie z. B. Smartphones im Privatbesitz? Es gibt zwar Unterschiede, aber die folgenden Punkte gelten für registrierte und nicht verwaltete Geräte:

- In beiden Fällen gibt es Schwachstellen.
- Beide enthalten sensible Daten.
- Alle müssen verwaltet werden.
- Sie alle benötigen risikogesteuerte Zugriffsrichtlinien in Echtzeit, um den Sicherheitstraum zu verwirklichen, Apps und Geschäftsdaten nur autorisierten Benutzer*innen zugänglich zu machen.

Daher gibt es nur eine Möglichkeit, Ihre Infrastruktur umfassend zu schützen: Sie müssen sich beider App-Typen bewusst sein und mehrschichtige Sicherheitsmaßnahmen implementieren, die sowohl webbasierte als auch geräteinterne Apprisiken abdecken.

Durch die Implementierung eines stärker integrierten IT-Programms, das die Funktionen der Geräte- und Appverwaltung mit den Fähigkeiten und Erkenntnissen von Sicherheitstools verbindet, können Unternehmen einen widerstandsfähigeren Arbeitsplatz schaffen. Der Schlüssel dazu ist eine umfassende Sicherheitsstrategie, die einen ganzheitlichen Schutz für Ihre gesamte Infrastruktur bietet, indem sie kompensierende Kontrollen einbezieht, um sich an Änderungen der Risikolage des Geräts anzupassen. Gleichzeitig werden die Geschäftsdaten über sichere Tunnel geleitet, die für jede Anfrage nach webbasierten Apps einzigartig sind.

Eine weitere Ebene der Sicherheitskontrolle verbindet die oben genannten Aspekte mit der Verwaltung und erzwingt die Compliance mit gehärteten Konfigurationsprofilen, verwalteter App-Bereitstellung und automatisierten Workflows zur Behebung von Schwachstellen, um eine Basislinie zu schaffen und ein grundlegendes Maß an Gerätesicherheit zu implementieren, unabhängig vom Gerätetyp, Eigentumsmodell oder der verwendeten Netzwerkverbindung, um produktiv zu bleiben.

Die wichtigsten in der Cloud gehosteten Geschäftsapps im Einsatz

Microsoft

Google

Dropbox

Adobe

Box

Slack

Okta

Atlassian

Salesforce

Zoom

Verwaltung von Schwachstellen und Risiken

Das kostenlose Herunterladen einer kommerziellen App ist zwar für manche verlockend, aber oft ist damit weit mehr verbunden, als die Nutzer*innen beim Erwerb von Apps aus App-Stores von Drittanbieteren erwartet haben. Für einen detaillierteren Blick auf die einzelnen Plattformen hat die Jamf Forschung herausgefunden, dass die Zahl der Downloads von Drittanbieter-Apps für Android doppelt so hoch ist wie für iOS.

Auch wenn Apple seine Sicherheits- und Datenschutzmaßnahmen in der gesamten Hardware- und Software-Produktpalette verdoppelt, zeigen diese Ergebnisse, dass das Unternehmen nicht immun gegen die Bedrohungstrends ist, die es zunehmend ins Visier nehmen.

„Android hat 2x mehr Downloads von Drittanbieter-Apps als iOS”

Sicherheit von Unternehmensdaten und modernen Geräten

Die Datensicherheit liegt an der Schnittstelle zwischen Work-Life-Balance und den mobilen Technologien, die Remote-/Hybridarbeit möglich machen. Als Teil einer Matrix betrachtet, zeigen die Scheitelpunkte, die zwei Punkte miteinander verbinden, in einigen Fällen auch ihre Ungleichheit zueinander. Zum Beispiel ein Gerät, das von einer medizinischen Fachkraft bei Hausbesuchen verwendet wird. Die auf dem Gerät gespeicherten Patientendaten oder geschützten Gesundheitsinformationen (Protected Health Information, PHI) unterliegen in den USA den Bestimmungen des HIPAA. Ein mobiles Gerät erleichtert dem Fachmann das Reisen (was das eine Ende der Scheitelpunkte darstellt), während es für böswillige Akteure relativ einfach ist, das Gerät selbst zusammen mit den darauf gespeicherten Daten zu stehlen (was das andere Ende der Scheitelpunkte darstellt). Einfacher ausgedrückt: Je leichter das Gerät für Benutzer*innen zu tragen ist, desto leichter fällt es einer unbefugten Person, es zu stehlen.

Größere Leichtigkeit = größeres Risiko.

Moderne Geräte müssen nicht unbedingt unternehmenseigene oder vom Unternehmen ausgegebene Geräte sein. Aufgrund verschiedener Faktoren, wie z. B. Verfügbarkeit von Geräten und Kosten für Softwarelizenzen, Wahlmöglichkeiten für Mitarbeiter*innen und Benutzerfreundlichkeit, sind moderne Arbeitsgeräte oft eine Mischung aus persönlichen und vom Unternehmen zur Verfügung gestellten Geräten und Apps. Unternehmen, die moderne IT- und Sicherheitsstandards anwenden, müssen unbedingt sicherstellen, dass nur autorisierte Benutzer*innen mit zugelassenen Geräten, die den Anforderungen des Unternehmens entsprechen, auf sensible Ressourcen und Apps zugreifen können.

Einer der wichtigsten Trends, der sich auf die Sicherheit von Unternehmensdaten auswirkt, betrifft daher die Risiken, die damit verbunden sind:

- Bring Your Own Device (BYOD)-Modelle
- Schatten-IT

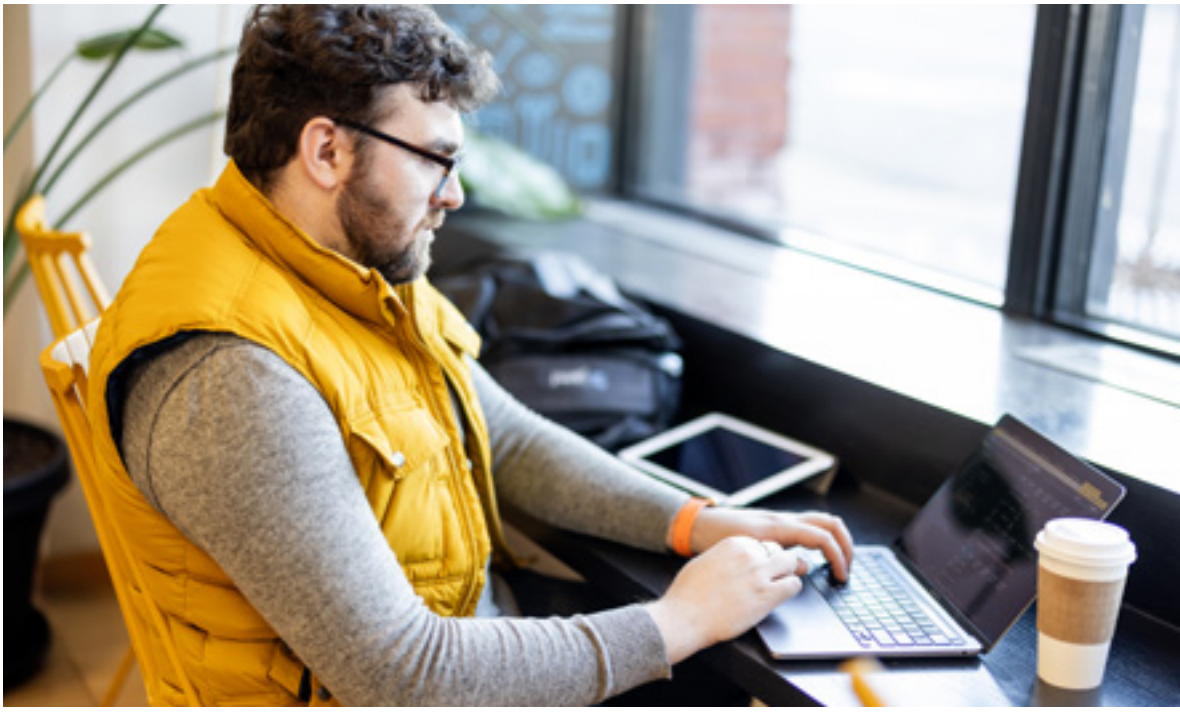
Beide Konzerne haben mit Geräten aller Art zu tun, die sich über mehrere Plattformen erstrecken und von Benutzer*in zu Benutzer*in unterschiedlich sind, um mit der von den Benutzer*innen gewählten Hardware und Software so produktiv wie möglich zu sein. Die Befähigung der Benutzer*innen ist ein entscheidender Aspekt der Produktivität. Dennoch zeigt dieser Mangel an Standardisierung, dass die Datensicherheit letztlich den Preis zahlt, wenn verschiedene Software-Tools und -Dienste - alle mit unterschiedlichen Risikofaktoren - in den Mix kommen. Webbrowser wie Google Chrome, Microsoft Edge und Mozilla Firefox erfüllen beispielsweise eine wichtige Funktion, indem sie Websites darstellen, auf denen Nutzer*innen praktisch jede Minute des Tages recherchieren und arbeiten können. Doch mehrere Apps multipliziert mit unterschiedlichen Versionen jeder App sowie mit den Common Vulnerabilities and Exposures (CVE), die mit jeder Version verbunden sind, ergibt eine unkalkulierbare Anzahl von Schwachstellen, die in der gesamten Geräteflotte vorhanden sind, für den Zugriff auf Unternehmensressourcen verwendet wird und wiederum Geschäftsdaten auf zahllosen Geräten verarbeiten, die weltweit für Arbeit und Schule genutzt werden.

Schatten-IT ist ihnen seit langem ein Dorn im Auge, denn die Nutzer*innen umgehen die Sicherheitsvorkehrungen, indem sie z. B. Sideloading-Apps verwenden oder sich auf ihre bevorzugte Cloudbasierte App verlassen, die möglicherweise nicht vollständig geprüft oder für die Verwendung mit Geschäftsdaten zugelassen ist, da die Verwendung unsicherer App-Versionen mit Risiken verbunden ist. Unsere Untersuchung zeigt, dass Onion Browser und Tor zu den am häufigsten auf Arbeitsgeräten installierten Apps gehören. Auf privaten Geräten, bei denen die Nutzer*innen selbst bestimmen können, welche Apps sie herunterladen und auf ihren Geräten verwenden möchten, waren Messenger-Apps, die mit Social-Media-Plattformen **verknüpft sind, in der Top-20-Liste der gefährdeten Apps zu finden, was zweifellos auf den wachsenden Trend zurückzuführen ist, dass Bedrohungsakteur*innen** ihre Opfer über soziale Medien durch betrügerische Stellenanzeigen ausnutzen. Diese gefälschten Profile kommunizieren direkt mit den Zielpersonen über Direktnachrichten, Betrügereien mit Kryptowährungsinvestitionen oder verbreiten ganz allgemein Fehlinformationen, die legitim erscheinen, es aber in Wirklichkeit nicht sind.

Die Überwachung von Schatten-IT ist eine Form der Compliance Verwaltung, die für Unternehmensgeräte relevant ist. Bei privaten Geräten wollen wir nicht nur sicherstellen, dass die Geräte ordnungsgemäß konfiguriert und einsatzbereit sind, sondern auch, dass die Richtlinien, die beispielsweise den Datenfluss zwischen geschäftlichen und privaten Apps regeln, gemäß den Standards des Unternehmens verwaltet werden.

Die übergreifende Botschaft ist, dass IT- und Sicherheitsteams die Aufgabe haben, Unternehmensressourcen zu sichern und den Zugang auf autorisierte Benutzer*innen zu beschränken. Die Mischung der Geräte - von Geräten, die vom Unternehmen zur Verfügung gestellt werden, bis hin zu privaten Geräten - sind jedoch Variablen, die sich auf die Sicherheit auswirken. Ein noch größeres Risiko stellen Apps dar, für die Unternehmen einen offenen Zugang gewähren, sodass sie von jedem Ort aus zugänglich sind. Dies umschließt auch Geräte, die nicht für die Arbeit bestimmt sind, da sie die Benutzer*innen nicht von ihrer Produktivität abhalten wollen. Um die Situation noch weiter zu verschlimmern, wurde festgestellt, dass einige Mitarbeiter*innen in dem Bestreben, sich das Leben zu erleichtern, die Arbeitsrichtlinien umgehen. Wenn das Arbeitsnetzwerk beispielsweise den Zugriff auf einen Dienst (z. B. Cloud Speicher A) blockiert, weil es den Speicherort von Arbeitsdaten in der Cloud einschränken möchte, Mitarbeitende jedoch ein persönliches Gerät verwenden, um sensible Dokumente in einem anderen Dienst (z. B. Cloud Speicher B) abzulegen, haben diese gegen die Richtlinie verstoßen und die Daten gefährdet.

Aus diesem Grund empfiehlt es sich, Richtlinien zu implementieren, die Benutzerauthentifizierung, Gerätebewertung und sichere Konnektivität miteinander verbinden, d.h. die Überbrückung der Lücke zwischen Verwaltung, Identität und Sicherheit durch mehrschichtigen Schutz in einer Defense-in-Depth-Strategie, die Geräte, Benutzer*innen und Daten auf jeder Ebene schützt und verwaltet, unabhängig von Gerätetyp, physischem Standort, Eigentumsmodell, Betriebssystemplattform oder Netzwerkverbindung.



Abschnitt III: Malware-Analyse und Angriffsentwicklung

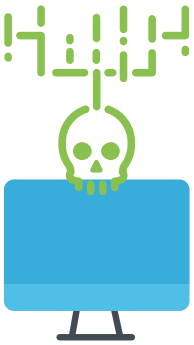
In diesem Abschnitt gehen wir detailliert darauf ein, welche Malware-Bedrohungen im Jahr 2023 die größten Auswirkungen auf Unternehmen haben und wie häufig sie in freier Wildbahn auftauchen. Außerdem gehen wir auf die kontinuierliche Entwicklung von Angriffen ein, die beide Plattformen betreffen, und darauf, wie böswillige Akteur*innen Schwachstellen in Tools auf Betriebssystemebene ausnutzen, um Benutzer*innen ein falsches Sicherheitsgefühl vorzugaukeln (mehr dazu später in diesem Abschnitt).

macOS Bedrohungen

Benutzer*innen mögen die Augen vor den Risiken verschließen, denen sie online ausgesetzt sind, aber Unternehmen wissen, dass die zunehmende Nutzung von Geschäftsapps ihre Benutzer*innen gezielter denn je macht.

Wussten Sie, dass

„57 % der Mac Nutzer*innen der Aussage „Malware gebe es nicht auf macOS" entweder zustimmen oder zögern dabei, ihr nicht zuzustimmen?
Laut **Umfrageergebnissen von The Hacker News**, glaubt im Jahr 2023 „jede/r dritte Mac Nutzer/in, dass seine/ihre Daten für Cyberkriminelle uninteressant seien."



21

neue Malware-Familien auf dem Mac

Der Mythos, dass es für Mac keine Viren gibt, hält sich hartnäckig, doch Jamf Threat Labs verfolgt rund 300 Malware-Familien unter macOS. Im Jahr 2023 gab es sogar 21 neue Malware-Familien für Mac!

Im Folgenden finden Sie eine vollständige Aufschlüsselung der untersuchten und gezählten neuen Mac Malware-Instanzen im Jahr 2023, basierend auf unseren Erkenntnissen:

Malware Kategorie	% der gesamten Mac Malware
Adware	36,77
PUA	35,24
Trojaner	17,96
Exploit	4,40
Ransomware	2,00
Downloader	0,92
Hacktool	0,67
Coinminer	0,64
Zertifikate	0,64
Dropper	0,56
Infostealer	0,25
Spionageprogramme	0,23
Malware	0,20
Keylogger	0,04
Netzwerk	0,026
Virus	0,01
Rogue	0,01
Hyperlink	0,01

Wie Sie aus der Aufschlüsselung ersehen können, ist jede Kategorie in der Reihenfolge des höchsten Anteils an Mac Malware bis zum niedrigsten aufgelistet. Im Folgenden finden Sie einige interessante Daten zu einigen der von uns entdeckten Malware-Funde. Bei PUA, den potenziell unerwünschten Apps, ist es schwierig, diese Kategorie zu quantifizieren, da es sich um eine App handeln könnte, die von Benutzer*innen wissentlich installiert wurde und ansonsten harmlos ist, oder um etwas, das während der Installation absichtlich vor Benutzer*innen versteckt wurde, um seine Erkennung zu verschleiern. Aufgrund dieser Variablen müssen die Benutzer*innen wachsam sein, was unbeabsichtigte Aktionen auf ihrem Mac angeht.

Im vergangenen Jahr wurden Trojaner mit der höchsten Anzahl von Familien beobachtet. Dies deutet auf eine große Vielfalt bei der Verpackung und Verbreitung dieser Art von bösartigem Code hin, was möglicherweise auch ein Indikator für eine größere Anzahl von Malware Autor*innen ist. **Mit 17 % stellt die Kategorie „Trojaner"** ein erhebliches Risiko dar, das in der macOS Malware-Community immer beliebter wird. Überlegen Sie: Was fügen die Bösewichte in die Systeme ein? Warum wenden sie diese Taktik an? Schließlich handelt es sich bei Trojanern per Definition um Software, in der andere schädliche Programme versteckt sind. Dies unterstreicht nicht nur die Notwendigkeit einer Schwachstellenverwaltung, sondern auch:

- Bewerbungen aus seriösen Quellen zu erhalten
- Apps eines Überprüfungsprozesses (entweder durch vertrauenswürdige Dritte wie Apples App Store oder durch das eigene Sicherheitsteam einer Organisation) zu unterziehen
- des Einsatzes aktueller Sicherheitssoftware

Atomic Stealer

Der auf Telegram beworbene Atomic Stealer arbeitet als Malware-as-a-Service mit einer Web-Schnittstelle für Angreifer*innen. Er ist auf Informationsdiebstahl spezialisiert und kann eine Reihe sensibler Daten exfiltrieren, z. B. Kontopasswörter, Browserdaten, Sitzungscookies und Kryptowährungs-Wallets. Atomic missbraucht insbesondere AppleScript Dialogfunktionen, um Benutzer*innen zur Eingabe ihrer Anmeldedaten zu verleiten. Sobald das Passwort des Benutzers/der Benutzerin eingegeben ist, stiehlt er weitere sensible Daten aus dem macOS Schlüsselbund. Die Malware wird unter dem Deckmantel legitimer Apps wie Tor Browser, Photoshop CC, Notion und Microsoft Office verbreitet und wurde auch über Malvertising in Google Ads beworben.

JokerSpy

JokerSpy wird der APT-Gruppe BlueNoroff zugeschrieben und wurde zuerst bei einer Kryptowährungsbörse in Japan entdeckt. Die Malware nutzt eine Reihe von Hintertüren, um Spionagesoftware auf kompromittierten Systemen zu installieren, und verwendet Open-Source-Tools zur Aufklärung. Seine in Python geschriebenen Hintertüren ermöglichen das dynamische Laden von Konfigurationen und die Ausführung von Befehlen, was eine Vielzahl von bösartigen Aktionen ermöglicht. JokerSpy wertet nicht nur die Systemberechtigungen aus, sondern ist auch dafür bekannt, Apples Einstellungen für Transparenz, Zustimmung und Kontrolle (TCC) zu missbrauchen. Es kann auch SwiftBelt einsetzen, ein Open-Source-Toolset für macOS, das häufig in Red-Teaming-Übungen verwendet wird.

KandyKorn

Diese Malware wurde als Teil eines weitaus größeren, raffinierteren Angriffs entdeckt, bei dem nordkoreanische Bedrohungsakteur*innen auf Blockchain-Ingenieur*innen abzielten. Die Angreifer*innen führten einen mehrstufigen Malware-Angriff über einen gefälschten Bot auf Discord durch. Die anfängliche Kompromittierung umfasste verschiedene bösartige Python-Skripte, die zusätzliche Malware-Komponenten herunterluden. Anschließend dienten die Python-Skripte als Dropper für die nächste Stufe der Malware, die eine Verbindung zu einem C2-Server herstellte. Danach wurde eine weitere Malware-Stufe eingesetzt, die Persistenz- und Verteidigungsumgehungstechniken wie das reflektierende Laden von Binärdateien verwendete, was letztendlich zur speicherinternen Ausführung der KandyKorn-Malware führte.

Lockbit

VXUnderground spricht von einem Meilenstein - dem ersten Fall einer großen Ransomware-Gruppe, die es auf Apple Produkte abgesehen hat. LockBit scheint eine Apple Portierung seines Linux-Gegenstücks zu sein und tauchte erstmals Anfang 2022 auf. Die ersten Beispiele zeigten eine Ad-hoc-Signatur, die bei der Ausführung ein Popup-Fenster mit einer ungültigen Signatur auslöste. Nach neuesten Informationen exfiltriert LockBit noch keine Daten und befindet sich vermutlich in aktiver Entwicklung, was darauf schließen lässt, dass weitere Funktionen folgen könnten. Bei erfolgreicher Ausführung verschlüsselt die Ransomware Dateien mithilfe von Open-Source-Bibliotheken und hinterlässt eine Lösegeldforderung im Dateisystem.

NokNok

Bei NokNok handelt es sich um eine APT-Malware-Kette, die einem iranischen Bedrohungsakteur zugeschrieben wird und für die Aufklärung und den Einsatz von Backdoors auf den Systemen der Opfer entwickelt wurde. Die Angreifer*innen verwenden gezielte Phishing-E-Mails, die sich als Royal United Services Institute (RUSI) ausgeben und die Opfer dazu verleiten, eine bösartige VPN-App herunterzuladen, die den Namen RUSI trägt. Nach der Installation nutzt NokNok Bash-Skripte, um Hintertüren einzurichten und Serverbefehle zu empfangen, die entweder zur Selbstbeendigung oder zur Ausführung zusätzlicher Module führen können. Diese Module sammeln Daten über laufende Prozesse, Systeminformationen und installierte Apps und können auch die Persistenz sicherstellen. Für die sichere Datenübertragung setzt NokNok seine eigene Verschlüsselung ein, die durch base64-Kodierung und Segmentierung weiter verschleiert wird.

iWebUpdate

iWebUpdate ist ein persistenter Downloader, der entwickelt wurde, um beliebige Nutzdaten von einem entfernten Server zu holen und auszuführen. Es erhält die Persistenz durch einen Benutzer-Start-Agenten namens iwebupdate.plist. Nach der Aktivierung führt er Erkundungen durch, indem er Befehle wie system_profiler ausführt, um Informationen über die Betriebssystemversion zu sammeln, die dann an einen Befehls- und Kontrollserver gesendet werden. Die Nutzdaten werden in eine temporäre Datei unter /tmp/iwup.tmp heruntergeladen, entpackt und anschließend ausgeführt. Die Malware meldet sich stündlich beim Server, um weitere Aufgaben zu erledigen.

ObjCShellz

ObjCShellz, eine Objective-C-Backdoor, die der APT-Gruppe BlueNoroff/Lazarus zugeschrieben wird, ermöglicht es Angreifer*innen, Shell-Befehle an kompromittierte Systeme zu senden. Nach dem Aufbau einer Verbindung mit seinem Command-and-Control-Server erlaubt er die Ausführung von Shell-Befehlen, deren Ergebnisse an Angreifende zurückgesendet werden. Diese Malware wurde erstmals von Jamf Threat Labs im Rahmen der RustBucket-Kampagne identifiziert, einer BlueNoroff-Operation, die häufig auf kleine, auf Kryptowährungen spezialisierte Unternehmen abzielt.

PureLand

PureLand ist eine Malware, die Informationen stiehlt und in eine raubkopierte Version des legitimen Indie-Videospiels „PureLand" eingebettet ist. Das per E-Mail verbreitete trojanisierte Spiel verspricht den Nutzer*innen, beim Spielen Kryptowährung zu generieren. Bemerkenswert ist, dass PureLand zeitgleich mit Realst Stealer entdeckt wurde, einer anderen Malware, die eine auffallend ähnliche Social-Engineering-Taktik anwendet, aber eine andere endgültige Nutzlast aufweist.

Realst Stealer

Realst Stealer, eine auf Rust basierende Malware, die sich auf den Diebstahl von Informationen konzentriert, zielt in erster Linie auf Kryptowährungen auf kompromittierten Systemen ab. In einer gut dokumentierten Kampagne wurde die Malware auf raffinierte Weise in weniger bekannte Videospiele eingebettet. Um sie zu verbreiten, wandten sich die Angreifer*innen an Einzelpersonen und boten ihnen einen exklusiven, frühzeitigen Zugang zu diesen Spielen an und präsentierten sie als NFT-basierte Möglichkeit, Krypto zu verdienen. Sobald der Benutzer/die Benutzerin das Spiel startet, wird Realst Stealer aktiviert, kompromittiert das System und beginnt mit seinen Krypto-Diebstahlsroutinen.

Rustbucket

RustBucket ist ein Trojaner für den Fernzugriff. Trojaner sind oft eher auf Spionagefähigkeiten als auf finanziellen Gewinn ausgerichtet, aber je nach den Zielen der Angreifer*innen kann es zu gewissen Überschneidungen kommen. Sie enthalten in der Regel mehrere verschiedene Funktionen wie Remote-Shell-Funktionen, Keylogger, Infostealer und mehr.

Bei RustBucket, das von der APT-Gruppe BlueNoroff - einer nordkoreanischen Untergruppe der bekannten Lazarus-Gruppe - eingesetzt wird, handelt es sich um eine mehrstufige Malware, die Benutzer*innen über komplizierte Social-Engineering-Kampagnen anspricht. Die anfänglichen Dropper sind in Objective-C, Swift und AppleScript geschrieben, während die endgültige Nutzlast in Rust erstellt wird. In typischen Kampagnen tarnt sich die Malware als harmloser PDF-Reader. Die Benutzer*innen werden davon überzeugt, ein bestimmtes PDF-Dokument mit dieser bösartigen App zu öffnen, wodurch ein Rückruf an den Command-and-Control-Server des Angreifers/der Angreiferin ausgelöst wird.

WTFMiner

WTFMiner ist eine ausweichende Kryptojacking-Malware, die sich über raubkopierte macOS Apps verbreitet. Seine Ursprünge lassen sich auf einen Torrent-Uploader zurückführen, der den Miner seit 2019 in mehrere raubkopierte macOS Apps integriert hat. Durch die Beschaffung von Kopien konnte Jamf seine schrittweise Entwicklung über drei Generationen verfolgen, wobei jede Version zusätzliche Tarntechniken enthielt. Er verwendet Dark-Web-Routing für die verdeckte Kommunikation, tarnt sich als legitimer Prozess und fährt herunter, wenn die Aktivitätsanzeige geöffnet wird. Die neuesten Varianten vermeiden das Schreiben von Persistenzdaten auf die Festplatte und verlassen sich darauf, dass die Benutzer*innen die trojanisierten Anwendungen starten, um das Mining zu initiieren.

Schließlich haben unsere Untersuchungen ergeben, dass Ransomware trotz der niedrigsten Familienanzahl immer noch unter den ersten fünf auf der Liste der neuen Malware in freier Wildbahn zu finden ist, da eine beträchtliche Anzahl von Instanzen identifiziert wurde, die zu diesem Malware-Klassifizierungstyp gehören. Obwohl im letzten Jahr einige neue Ransomware-Familien entdeckt wurden, wie z. B. **Turtle Ransomware** und **Lockbit für macOS**, hat Jamf Threat Labs festgestellt, dass die meisten als „Ransomware" bezeichneten Muster weiterhin zur EvilQuest-Ransomware gehören, die ursprünglich im Jahr 2020 entdeckt wurde.

Obwohl dies interessant ist, sind viele der Meinung, dass die EvilQuest-Proben in erster Linie durch einen Sandbox-Fehler erzeugt werden, der weiterhin zu winzigen Unterschieden in den Proben führt. Die Ransomware wird nicht aktiv an die Opfer ausgeliefert und wurde seit ihrer Entdeckung im Jahr 2020 auch nicht ausgeliefert.

Was wir tatsächlich gefunden haben

Ein detaillierterer Blick auf neue Mac Malware, die in Kundenumgebungen beobachtet wurde, zeigt, dass die folgenden Malware-Familien unter den Top 10 rangieren:

Rang	Familie	% der insgesamt gesehenen in freier Wildbahn	Kategorie
1	genieo	13,63	Adware
2	imobie	12,25	PUA
3	generic	10,02	Adware
4	multiverze	6,84	Adware
5	tnt	6,19	PUA
6	ccleanmac	5,28	Adware
7	mackeeper	4,55	Adware
8	pirrit	4,45	Adware
9	macinformer	4,37	Adware
10	installcore	3,98	Adware

Mobile Bedrohungen

Trotz des Irrglaubens, dass Macs immun gegen Malware sind, sind mobile Bedrohungen, insbesondere auf Plattformen wie iOS, real und lassen sich nur schwer mit einfachen Statistiken quantifizieren. Sicherheitsexpert*innen sind mit den realen Auswirkungen dieser Bedrohungen auf die Unternehmensdaten und die Privatsphäre der Benutzer*innen konfrontiert. Im weiteren Verlauf des Abschnitts werden wir einige überraschende Entdeckungen von Sicherheitsforschern aus dem Jahr 2023 vorstellen, die die detaillierte Natur dieser mobilen Bedrohungen verdeutlichen.

Hinweis: Die in diesem Abschnitt angegebenen Prozentsätze, die auf unseren Erkenntnissen beruhen, erscheinen deutlich niedriger, insbesondere im Vergleich zu anderen Abschnitten in diesem Bericht. Aber wie ein Sprichwort sagt: „Der Schein trügt", was besonders im Bereich der Cybersicherheit von entscheidender Bedeutung ist, denn:

- Die **Weltbevölkerung hat nach Schätzungen der Vereinten Nationen im Jahr 2022** 8 Milliarden Menschen erreicht
- Bis zum Jahr 2023 wird die **Gesamtzahl der mobilen Geräte weltweit auf 16,8 Milliarden** geschätzt, Tendenz steigend
- Der Prozentsatz der **weltweiten Nutzer*innen mit einem Desktop- oder Laptop-Computer zu Hause** liegt bei 47,1 %, wie zuletzt im Jahr 2019 berichtet
- 3.6 ist **die durchschnittliche Anzahl von Geräten pro Person weltweit**.

Warum sind all diese Statistiken über Bevölkerungszahlen, Gerätetypen und durchschnittliche Geräte pro Person so wichtig, um die Auswirkungen moderner, mobiler Sicherheitsbedrohungen zu verstehen? Es ist ein wichtiger Kontext zu den Zahlen in unserer Forschung.

> „**<1 %** der Geräte und **2 %** der Unternehmen hatten im Jahr 2023 eine potenziell unerwünschte App in ihrer Geräteflotte installiert."

Wie bereits erwähnt, mag 1 % nicht sehr besorgniserregend erscheinen, und weniger als das ist, nun ja, weniger besorgniserregend, richtig?

Falsch. Hier werden die obigen Statistiken extrapoliert, um ein genaues, realistisches Bild davon zu vermitteln, wie kritisch diese Prozentsätze wirklich sind.

Beginnen wir mit den 16,8 Milliarden mobilen Geräten, die derzeit weltweit im Einsatz sind. Wenn wir 1 % davon ermitteln, bleiben 168.000.000 mobile Geräte mit installierter Malware übrig. Wenden wir uns nun der Weltbevölkerung von 8 Milliarden Menschen zu und entfernen die 47,1 % der Computernutzer*innen, um unsere Zahlen auf die mobile Nutzung zu beschränken. Dies ergibt eine Bevölkerung von 4,232 Milliarden potenziellen Nutzer*innen von Mobilgeräten. Zuletzt - und hier wird es knifflig - multiplizieren wir unsere verfeinerte Bevölkerungszahl mit dem weltweiten Durchschnitt von 3,6 mobilen Geräten pro Nutzer*in und kommen so auf 15,23 Milliarden mobile Geräte.

Nun muss man kein Mathegenie sein, um zu erkennen, dass 15,23 Milliarden weniger sind als 16,8 Milliarden. Hier kommt der knifflige Teil ins Spiel. Der globale Durchschnitt ist genau das: eine Zahl, die den Durchschnitt aller einzelnen Regionen bildet, um eine einzige globale Kennzahl zu ermitteln. Jede Region hat jedoch unterschiedliche Ausgangswerte, einige liegen unter dem weltweiten Durchschnitt, wie die Region Lateinamerika (3,1), während andere Regionen im Durchschnitt das Drei- bis Vierfache des weltweiten Durchschnitts erreichen, wie Westeuropa (9,4) und Nordamerika (13,4). Wenn wir die Zahlen noch einmal überprüfen, um regionale Schwankungen auszugleichen, kommen wir zu den folgenden Zahlen für die oben genannten Regionen:

- Lateinamerika: 11.680.800.000
- Westeuropa: 35.419.200.000
- Nordamerika: 50.491.200.000

Das letzte bisschen Mathe, versprochen! Lassen Sie uns nun noch einmal betrachten, was 1 % der mit Malware infizierten Mobilgeräte bedeutet, wenn man die nach Regionen bereinigten Werte hochrechnet:

- Lateinamerika: 116.808.000
- Westeuropa: 354.192.000
- Nordamerika: 504.912.000

Denken Sie daran, dass jedes Gerät - und sei es *nur* ein einziges kompromittiertes - ausreicht, damit böswillige Akteur*innen eine Datenverletzung erfolgreich durchführen können.

Angriffsentwicklung

2023 bot dem Team von Jamf Threat Labs außergewöhnliche Möglichkeiten bei der Entdeckung nicht nur einer, sondern mehrerer unterschiedlicher, komplexer und dennoch leistungsstarker mobiler Bedrohungen, die alle auf iOS basierte Mobilgeräte und deren Benutzer*innen abzielen.

Und obwohl mobile Geräte aus mehr als nur der Apple Plattform bestehen, deutet ein großer Teil unserer Untersuchungen auf wachsende Trends hin, die die Position unterstreichen, dass Bedrohungsakteur*innen zunehmend das Apple Ökosystem ins Visier nehmen und beträchtliche technische Ressourcen auf die Entwicklung neuartiger und schwer zu entdeckender Angriffe zur Kompromittierung der iOS/iPadOS Plattformen verwenden.

Apple hat in dieser Hinsicht eine Vorreiterrolle eingenommen, indem es die Sicherheit und den Schutz der Privatsphäre zu einem wesentlichen Bestandteil seiner Designphilosophie gemacht hat. Laut der Studie **Mobile Bedrohungen für Verbraucher- und Unternehmensdaten** hat sich *die Gesamtzahl der Datenschutzverletzungen zwischen 2013 und 2022 mehr als verdreifacht, wobei allein in den letzten zwei Jahren 2,6 Milliarden personenbezogene Daten preisgegeben wurden, und sie stellen fest, dass sich die Situation im Jahr 2023 weiter verschlechtern wird.*

Entwicklung des Social Engineering

Mobile Bedrohungen sind sehr real. Viele neue Apps und Dienste von Drittanbietern werden von Jahr zu Jahr verbreiteter und fortschrittlicher. Unser Jamf Threat Labs Team hat einige neue Sicherheitsbedrohungen für iOS im Jahr 2023 gefunden, die als Social Engineering 2.0 bezeichnet werden und diesen Trend belegen.

Pegasus-Entdeckungen

Im April veröffentlichte Jamf Threat Labs eine Untersuchung von zwei Geräten, die durch Pegasus kompromittiert wurden. Das erste, ein iPhone 12 Max Pro, das einem Menschenrechtsaktivisten im Nahen Osten gehörte, erwies sich als „eine Fundgrube für unsere Analyse, da es eine Reihe von Kompromissindikatoren enthielt und eindeutig mit Pegasus in Verbindung gebracht werden konnte."
Die Ergebnisse zeigten „eindeutige Indikatoren für eine Kompromittierung (IOCs) und Beweise für aktive Spyware-Kampagnen."

Außerdem entdeckte Jamf bei der Analyse des Dateisystems des zweiten Geräts, eines iPhone 6s, das einem bei einer globalen Nachrichtenagentur in Europa tätigen Journalisten gehörte, einen neuen IOC. Ihre Untersuchung ergab, dass Bedrohungsakteur*innen weiterhin ältere Geräte ins Visier nehmen, was sie daran erinnert, dass sie vor nichts zurückschrecken, um „Schwachstellen in der Infrastruktur eines Unternehmens auszunutzen und anzugreifen, wo immer es möglich ist."

Gefälschter Flugzeugmodus

Im August entwickelte Jamf Threat Labs eine Post-Exploit-Technik, um die Persistenz von iOS 16 zu erreichen. Indem er die Benutzeroberfläche so bearbeitet, dass die entsprechenden Bildschirmsymbole angezeigt werden, während er gleichzeitig die Internetverbindung zu allen Apps unterbricht, gaukelt ein Angreifer/eine Angreiferin den Benutzer*innen vor, dass der Flugzeugmodus aktiviert ist, während er in Wirklichkeit den Netzwerkzugriff auf das Gerät auf ausgenutzten oder jailbroken iPhones aufrechterhält.

Der Flugzeugmodus bietet einen zusätzlichen Schutz der Privatsphäre und die Compliance während der Reise, was sicherheits- und datenschutzbewusste Benutzer*innen beruhigt. Durch die Modifizierung und damit Unterbrechung dieser Funktionalität könnten die Geräte der Opfer dieses Angriffs jedoch unbemerkt kompromittiert werden, während potenzielle Bedrohungsakteur*innen auf ihrem Weg durch die Angriffskette eine Persistenz erreichen und den unbefugten Zugriff auf die betroffenen iOS basierten Geräte aufrechterhalten.

Gefälschter Sperrmodus

Im Dezember entwickelte Jamf Threat Labs eine neue Technik, die auf den bereits erwähnten Proof of Concept zurückgeht. Diese Methode hat größere Auswirkungen auf die Sicherheit und den Schutz der Privatsphäre der Nutzer*innen. Diese Manipulationstechnik konzentriert sich auf den Lockdown-Modus von Apple und bietet alle visuellen Hinweise, die mit einem funktionierenden Lockdown-Modus in Verbindung gebracht werden, ohne die Schutzmaßnahmen, die normalerweise von dem Dienst implementiert werden.

Angreifer*innen, die das Gerät kompromittieren, könnten bösartigen Code einschleusen, um den hier beschriebenen Angriff durchzuführen. Bei der Aktivierung des Lockdown-Modus lösen Benutzer*innen mit hohem Risiko auf einem anfälligen Gerät versehentlich den Code von Angreifenden aus, der die visuellen Hinweise des Lockdown-Modus implementiert, aber keine Änderungen an der Konfiguration des Geräts vornimmt. Anstelle des Schutzes und der Minimierung der aus der Ferne zugänglichen Funktionen ist das Ergebnis ein iPhone, von dem Endbenutzer*innen glauben, dass es bis zu einem gewissen Grad geschützt ist, während es in Wirklichkeit ungeschützt, kompromittiert und für Bedrohungsakteur*innen voll zugänglich ist.

Abschnitt IV: Internet-Bedrohungen und Online-Risiken

Angriffe, die die Vernetzung moderner Geräte ausnutzen - um Benutzer*innen oder das Gerät über das Netzwerk anzugreifen, Befehls- und Kontrollsignale zu übermitteln oder Daten zu exfiltrieren - werden als webbasierte Bedrohungen eingestuft. Dieser Oberbegriff beschreibt verschiedene Bedrohungen und nicht nur eine Art. Diese Art von Bedrohung ist auch für einige der größten, raffiniertesten, tödlichsten und - zum Leidwesen ihrer Opfer - erfolgreichsten Angriffe in der modernen Bedrohungslandschaft verantwortlich.

Web-Bedrohungen sind ein sehr wichtiger und strategischer Teil der Angriffskette für mobile Geräte. Ein gemeinsamer Ausgangspunkt, der ein breites Spektrum an Nutzer*innen und Geräten abdeckt. Vielleicht ist es etwas anderes als CVE-Exploits in einer App oder einem Betriebssystem, aber es ist ein wichtiger Teil einer Angriffskette, über die Unternehmen eine starke Kontrolle haben, wenn sie sich entscheiden, sie zu implementieren

Wir sollten Web-Bedrohungen nicht als „Alternative" zu anderen Bedrohungsvektoren behandeln. Es ist einfach ein Lieferfahrzeug. Diese Angriffe werden oft mit herkömmlichen Taktiken kombiniert, um einen erfolgreichen Angriff zu starten. Dies sind alles Teile eines größeren Puzzles, das oft:

1. den Bedrohungsakteur*innen mit dem geringsten Aufwand den größtmöglichen Erfolg verschafft;
2. dafür sorgt, dass selbst die strengsten Sicherheitsrichtlinien und -kontrollen umgangen werden können.

Wenn man sich die erste Hälfte der Antwort genauer ansieht, braucht man keine Kristallkugel, um zu wissen, dass die größte Bedrohung nach wie vor das Phishing ist. Das Versenden eines bösartigen Links per SMS an Hunderte oder Tausende von Zielpersonen dauert nur wenige Sekunden, und die Wahrscheinlichkeit, dass zumindest einige der Zielpersonen darauf klicken, ist hoch genug, um die Kampagne erfolgreich zu machen.

Die zweite Hälfte der Antwort ist eindeutig: Alle Sicherheitskontrollen der Welt nützen nichts, wenn die Benutzer*innen ihre Anmeldedaten und damit den Zugang zu personenbezogenen Daten einfach weitergeben. Es ist keine technische Zauberei im Spiel, und es muss auch kein komplexer Code entwickelt werden - es genügt, die Zielperson auf halbwegs überzeugende Weise aufzufordern, ihre Anmeldedaten anzugeben, um ein System oder einen Dienst zu kompromittieren.

Im Folgenden werden die wichtigsten Bedrohungen für Geräte näher beleuchtet.

Phishing

Wie bereits erwähnt, ist Phishing die größte Bedrohung und das aus gutem Grund: minimaler Aufwand für maximalen Erfolg.

9 %
der Nutzer*innen fielen auf einen Phishing-Angriff herein

und Phishing-Angriffe auf mobilen Geräten waren 50 % erfolgreicher als auf Macs.

Die schlechte Nachricht zuerst: Dies ist ein Anstieg um 1 % gegenüber 2022, als 8 % der Nutzer*innen auf einen Phishing-Angriff hereinfielen.

Dies bedeutet, dass Unternehmen zwar über einen besseren Schutz und eine bessere Ausbildung in Bezug auf die Datensicherheit zu verfügen scheinen, dass aber die Zahl der Kompromittierungen bei den einzelnen Benutzer*innen zunimmt. Dies entspricht dem Trend, dass Angreifende die Benutzer*innen direkt und aggressiver über andere Kanäle wie soziale Medien ins Visier nehmen, wobei sie zweifelsohne von den Remote-/Hybrid-Arbeitskräften profitieren, die persönliche Geräte für ihre Arbeit nutzen. Im Jahr 2023 waren Phishing-Angriffe auf mobilen Geräten 50 % erfolgreicher als auf Macs. Und da laut **CISA** „mehr als 90 % aller Cyberangriffe mit Phishing beginnen", ist es nicht verwunderlich, dass böswillige Akteure*innen die primären Geräte der Benutzer*innen als Sprungbrett nutzen, um von persönlichen Daten auf Geschäftsdaten überzugehen.

„Kryptojacking 1 % der Geräte und 9 % der Unternehmen."

Während die Cybersicherheitsbranche bereits 2011 vor Kryptojacking gewarnt wurde, wurde der erste wirkliche Anstieg im Jahr 2022 gemeldet, als die Zahl der Vorfälle auf 140 Millionen stieg, was einem **Anstieg von 43 % weltweit** entspricht, wie Statista feststellt. Sonic Wall fand heraus, dass die Zahl der **Kryptojacking-Angriffe allein in der ersten Hälfte des Jahres 2023 um 399 % auf 332,3 Millionen** Vorfälle anstieg.

Wie weit verbreitet Kryptojacking ist, zeigen unsere Sicherheitsforscher*innen, als das Team von **Jamf Threat Labs Anfang 2023 in Raubkopien kommerzieller Software für macOS eingebettete Kryptojacking-Malware** identifizierte. Wie mehrere Forschungsarbeiten belegen, ist Kryptojacking nach wie vor ein gefährlicher Trend, auf den Bedrohungsakteur*innen im wörtlichen und übertragenen Sinne setzen. Es ist ein Problem, das Unternehmen ernst nehmen müssen, denn es geht längst nicht mehr nur um den Diebstahl von Ressourcen, sondern um kriminelle Handlungen, mit denen Bedrohungsakteur*innen eine Menge Geld verdienen und die sie und andere Cyber-Bedrohungen am Laufen halten.

Bösartiger Netzwerkverkehr
Nicht zu verwechseln mit der Installation von Malware (siehe unsere Analyse dieses Bedrohungstyps weiter unten im Bericht), stellt bösartiger Netzwerkverkehr eine erhebliche Bedrohung für „11 % der Geräte" in unserem gesamten Forschungspool dar. Auf Unternehmensebene haben wir festgestellt, dass 20 % der Unternehmen von bösartigem Netzwerkverkehr betroffen waren."

Beispiele für bösartigen Netzwerkverkehr sind:

- Malware-Download
- Befehl und Kontrolle
- Exfiltration von Daten
- Betrug
- Wenn man diesen Prozentsatz weiter aufschlüsselt, stellt man fest, dass Mobilgeräte mit Android und iOS 8 % bzw. 6 % der Gesamtzahl ausmachen Weitere bemerkenswerte Ergebnisse waren:
- **2 % der Unternehmen hatten ein Passwort-Leck** (Zugangsdaten wurden ohne Zustimmung online veröffentlicht)
- **1 % der Nutzer*innen waren mit einem riskanten Hotspot** verbunden (drahtlose Netzwerke, die ungesichert sind und oft kostenlos genutzt werden können)
- **Etwa 1 % war von MitM** (Man-in-the-Middle)-Angriffen betroffen (wenn Bedrohungsakteur*innen unabhängige Verbindungen zwischen zwei Opfern herstellen und Nachrichten zwischen ihnen weiterleiten, wobei diese oft verändert werden, um Daten zu sammeln)

Diese Prozentsätze sind zwar nicht die großen, aufsehenerregenden Zahlen, die in den Medien verbreitet werden, aber wenn man sie mit der Anzahl der Geräte in unserer Stichprobe in Beziehung setzt, sieht man, was diese bescheidenen Prozentsätze in realen Zahlen bedeuten.

- 300.000 Geräte hatten ein Passwort-Leck
- 150.000 Nutzer*innen waren mit einem riskanten Hotspot verbunden
- Knapp 150.000 waren von MitM-Angriffen betroffen

Diese Zahlen entsprechen mindestens 150.000 Möglichkeiten für Folgendes:

- Bedrohungsakteur*innen, die ein Gerät kompromittieren
  - Die Erfassung von Geschäftsdaten
  - Pivot-Angriffe auf andere Endpoints
  - Den Einbruch in ein Netzwerk oder einen Dienst
  - Geräte, die nicht der Compliance entsprechen
  - Verstöße gegen lokale, staatliche, bundesstaatliche und/oder regionale Vorschriften
  - Rechtliche Verantwortungsübernahme für die Folgen von Vorfällen
  - Die zivil- und/oder strafrechtliche Verfolgung
  - Unternehmen, in Verruf zu geraten
  - Die etwaige Beendigung von Partnerschaften
  - Den Verlust von Geschäftsmöglichkeiten
  - Betriebsschließung/Betriebsaufgabe

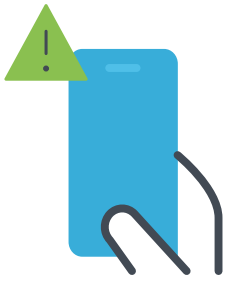
Geräte Compliance

Wir haben uns zwar mit jedem der drei Bedrohungstrends befasst, sind aber mit unseren Forschungsergebnissen noch nicht ganz fertig. In diesem Abschnitt konzentrieren wir uns jedoch nicht nur auf Bedrohungstrends, sondern auch auf Strategien zur Abschwächung von Bedrohungen, um die Geräte-Compliance besser aufrechtzuerhalten und Konfigurationsschwachstellen zu verwalten.

In diesem Bericht wird dies durch datengestützte Anleitungen auf der Grundlage unserer Forschungsergebnisse erreicht, die in drei spezifische Abschnitte unterteilt sind. Von diesen Abschnitten enthält jeder einzelne Bereiche, auf die sich IT- und Sicherheitsteams konzentrieren sollten, um eine ganzheitliche Compliance durch umfassende Verwaltungs- und Defense-in-Depth-Sicherheitsstrategien zu erreichen und zu erhalten.

Die Grundlagen

Unser erster Schwerpunktbereich gehört zu den kritischsten Abschnitten über die Geräte-Compliance, da er die Grundlage bildet, auf der die Instrumente und Strategien in den anderen Abschnitten aufgebaut werden. Wie der Titel schon andeutet, bilden einige Grundlagen den Antrieb für Ihren Sicherheitsplan, indem Sie sich auf die kritischen Funktionen konzentrieren, die sich immer wieder als Eckpfeiler für den Schutz Ihrer Endpoints erwiesen haben.



39 %

der Unternehmen hatten mindestens ein Gerät mit bekannten Sicherheitslücken

Patching und Sicherheits-Aktualisierungen

Jamf stellte fest, dass satte „39 % der Unternehmen mindestens ein Gerät mit bekannten Schwachstellen haben." Sicherheitsexpert*innen wissen, dass Zero-Day-Bedrohungen schwer zu erkennen und noch schwieriger zu entschärfen sind, da die Entwickler*innen noch keine Patches zur Neutralisierung dieser Art von Bedrohungen entwickelt haben. Aber wie die Ergebnisse zeigen, geht es hier um bekannte Schwachstellen oder solche, für die Patches verfügbar sind... nur fehlen den Geräten die entscheidenden Patches oder Aktualisierungen, um die Schwachstelle zu beheben.

Während sich die obige Feststellung auf alle Gerätetypen in den betroffenen Unternehmen bezieht, betrifft ein weiteres beunruhigendes Ergebnis die Nutzung mobiler Geräte: **„40 % der mobilen Nutzer*innen verwenden eine Betriebssystemversion mit bekannten Schwachstellen."** Dies ist ein eigenständiger Trend, da alle Beteiligten - nicht nur Unternehmen - für die Sicherheit ihrer Geräte verantwortlich sind. Gemeinsam spielen sie eine entscheidende Rolle bei der Feinabstimmung der Baselines für ihre Flotte durch iterative Workflows, um die Ringe bei neu veröffentlichten Betriebssystem-Aktualisierungen und App-Patches so schnell wie möglich zu schließen.

Als einer der Hauptgründe für Verzögerungen bei der Aktualisierung von Geräten wird die Angst vor Konflikten und zu vielen Agenten, die aktualisiert werden müssen, genannt.

Schnelle Sicherheitsreaktion (RSR)

In einer konzertierten Aktion zur Bekämpfung von Verzögerungen bei der Installation kritischer Sicherheits-Aktualisierungen auf Mac und iOS basierten Plattformen hat Apple Anfang 2023 Rapid Security Response eingeführt. Die Einführung von RSR optimiert die Bereitstellung kritischer Patches zur Risikominderung, indem der Download und die Installation auf unterstützten Geräten automatisiert werden. Apple Geräte und Benutzer*innen sind besser gegen die Einführung von Exploits geschützt, die in freier Wildbahn existieren, wenn sie den Abstand zwischen den großen Software-Aktualisierungen beachten.

macOS Security Compliance Project (mSCP)

Das Open-Source-Projekt mit dem Namen mSCP soll IT- und Sicherheitsteams, die mit der Verwaltung und dem Schutz von Apple Geräten betraut sind, dabei helfen, Sicherheitsbenchmarks zu implementieren, die mit ihren Compliance-Zielen übereinstimmen. Basierend auf den individuellen Compliance-Anforderungen Ihres Unternehmens bietet mSCP einen logischen, systematischen Ansatz für die Generierung von Konfigurations-Payloads und Einstellungen zur Durchsetzung der Compliance nach der Bereitstellung auf Ihrer Geräteflotte.

Die Rolle Verwaltung mit Blick auf Schutz

Verwaltung und Schutz stehen in einer symbiotischen Beziehung. Einfach gesagt: Das eine sollte nicht ohne das andere existieren. Der Endpoint-Schutz stellt sicher, dass die Geräte vor Bedrohungen geschützt sind, indem die Endpoints aktiv überwacht werden. Ohne Verwaltung wird die Behebung jedoch zu einem manuellen, zeitaufwändigen Aufwand, der umso schwieriger wird, je mehr Geräte Sie haben und je weiter entfernt diese sind. Umgekehrt können Verwaltungs-Workflows die Geräte-Compliance nicht automatisieren, wenn sie nicht über aktuelle Gerätetelemetrie verfügen, die aufzeigt, welche Mängel in Ihrer Flotte vorhanden sind.

Zu diesem Zweck ist der bereits erwähnte RSR von Apple ein solcher kritischer Patch-Service, der von der Verwaltung profitiert und der IT-Abteilung die Möglichkeit bietet, Geräte so zu konfigurieren, dass Sicherheitsreaktionen und Systemdateien automatisch auf den Geräten installiert werden, unabhängig davon, ob sie gesperrt oder abgemeldet sind.

Eine entscheidende Komponente in der Rolle der Verwaltung ist schließlich, wie die aktive Überwachung die Initiativen zur Compliance unterstützt. In Anlehnung an die Überlegungen zwischen nativen und cloudbasierten Apps im vorherigen Abschnitt bieten die aus der Überwachung gewonnenen Erkenntnisse der IT/Sicherheit einen Röntgenblick auf den Zustand eines Endpoints. Ausgestattet mit umfangreichen Telemetriedaten können diese Teams datengestützte Entscheidungen über die Sicherheit von Apps und die Datensicherheit treffen. Wie könnten Unternehmen ohne diese Daten den Sicherheitsstatus von Endpoints kennen, die z. B. aus der Ferne auf Webapps zugreifen?

Jamf Compliance Editor (JCE)

Jamf hat das Compliance-Tool auf der Grundlage von mSCP entwickelt und mit unseren MDM-Lösungen zu einer nativen macOS App kombiniert, die nicht nur benutzerdefinierte Compliance-Assets für Ihr Unternehmen generiert, sondern auch über eine in JCE integrierte Schnittstelle mit Ihrer Jamf Pro Instanz über eine sichere API verbunden ist, um Ihre neu generierten Assets hochzuladen. Dadurch wird die Lücke zwischen Generierung und Bereitstellung nahtlos überbrückt und Administrator*innen dabei geholfen, Zeit zu sparen, indem sie die Compliance schneller und effizienter durchsetzen.

Defense in depth

Kein Werkzeug ist narrensicher. Es gibt keine Patentlösung, die immer alle Bedrohungen abdeckt. Irgendwie, irgendwo, wird etwas versehentlich vorbeigehen. Das liegt in der Natur der Sache, aber das bedeutet nicht, dass es keine Maßnahmen gibt, die IT- und Sicherheitsteams ergreifen können, um das Risiko von Bedrohungen für Unternehmensressourcen zu minimieren. Das ist das Schöne an einem mehrschichtigen Schutz: Wenn eine Schicht es nicht auffängt, können die anderen Schichten es auffangen, bevor das Risiko zu etwas viel Schlimmerem wird.

Defense in Depth ist ein Sicherheitsparadigma, das über das einfache Zusammenschustern einer beliebigen Anzahl von Lösungen hinausgeht und das Unternehmen bei der Erstellung (oder Aktualisierung) ihres Sicherheitsplans anstreben sollten. Das Hauptziel besteht darin, verschiedene Lösungen in Schichten zu integrieren, wie eine Torte, bei der jede Schicht ein eigenes Sicherheitsinstrument ist, das aber auch als Sicherheitsnetz für die vorherige Schicht dient. Sollte es einer Bedrohung gelingen, an der nächsten Schicht vorbeizukommen, kann diese entschärft werden.

Trusted Access

Jamfs eigenes Sicherheitsparadigma ist ein hervorragendes Beispiel dafür, wie die Kombination der Lösungen Jamf Pro (Verwaltung), Jamf Connect (Identität) und Jamf Protect (Sicherheit) eine integrierte Plattform bildet, von der aus Administrator*innen die Verwaltung ihrer gesamten Flotte effektiv und ganzheitlich auf ihre Infrastruktur ausdehnen können, während gleichzeitig ein umfassender Sicherheitsschutz für Mac und mobile Geräte mit macOS, iOS/iPadOS/tvOS, Android und Windows bereitgestellt wird.

> „<1 % der Unternehmen hatten im Jahr 2023 ein jailbroken oder gerootetes Gerät."

Dieses Ergebnis ist ein Beweis dafür, dass weniger Nutzer*innen die für die Arbeit verwendeten Geräte jailbreaken/rooten, was eine gute Sache ist. Es ist jedoch auch ein Beweis dafür, dass die aktive Überwachung mobiler Geräte (Sicherheit) in Kombination mit dem Zero Trust Network Access (Identität), der dynamischen Durchsetzung von Sicherheitsrichtlinien und der automatischen Behebung von Problemen (Verwaltung) einen hervorragenden Arbeitsablauf darstellt, der verhindert, dass nicht konforme Geräte die Daten Ihres Unternehmens gefährden.

Mitarbeiterprogramme, die auf BYOD und COPE (Corporate Owned Personally Enabled) setzen, sind großartig für die Produktivität der Benutzer*innen, aber eine unzureichende Verwaltung und/oder übermäßige Sicherung der Geräte führt zu einer Reihe von Problemen, die sich auf die Datensicherheit und den Datenschutz der Endbenutzer*innen auswirken. Eine Lösung für den Mangel an Verwaltung und Schutz besteht darin, abgestufte Arbeitsabläufe zu implementieren, die sowohl firmeneigene als auch persönliche Geräte unterstützen, sodass beide Arten von Geräten eine grundlegende Sicherheitslage aufweisen.

So werden beispielsweise vom Unternehmen ausgegebene Geräte automatisch bei MDM mit Zero-Touch-Implementierung (Verwaltung) registriert, während persönliche Geräte von Benutzer*innen mit deren Anmeldedaten (Identität) registriert werden. Letztere haben ähnliche Konfigurationen wie erstere, mit dem Unterschied, dass ein geschäftliches Volume alle geschäftlichen Apps und Daten in einem verschlüsselten Volume speichert, das von dem persönlichen Volume getrennt ist, in dem die persönlichen Apps und Daten von Benutzer*innen gespeichert sind. Darüber hinaus wird der Datenschutz im Netz dadurch gewahrt, dass der gesamte geschäftliche Datenverkehr über verschlüsselte Mikrotunnel (Sicherheit) geleitet wird, während der private Datenverkehr direkt ins Internet geleitet wird. Schließlich bietet der Endpoint-Schutz sowohl für private als auch für unternehmenseigene Geräte das gleiche Maß an Bedrohungserkennung und -abwehr, da sie sich auf aktuelle Gerätezustandsdaten stützt, um den Gesundheitszustand des Endpoints bei jeder Anfrage zum Zugriff auf Unternehmensressourcen zu ermitteln. Auf der Grundlage des Null-Vertrauensmodells wird der Zugriff nur dann genehmigt, wenn ein Gerät verifiziert wurde. Schlägt die Verifizierung fehl, wird die Anfrage abgelehnt und ein automatischer Arbeitsablauf eingerichtet, um das Gerät zu korrigieren (Verwaltung). Danach wird erneut versucht, das Gerät zu verifizieren. Erst wenn dies der Fall ist, wird der Antrag genehmigt.

Die wichtigsten Erkenntnisse

- Einrichtung einer Verwaltung für alle Ihre Geräte - unternehmenseigene und BYOD-Geräte
- Verwendung von Endpoint-Schutz-Produkten zum Aufhalten von Malware und zum Sammeln von Telemetriedaten für weitere Analysen und die Bedrohungsjagd
- Angleichung an Compliance-Standards
- Implementieren Sie Sicherheit am Rande, inklusive der Geräte, die Ihren Unternehmenscampus verlassen
- Sichere Verbindung mit verschlüsselten Tunneln, um das Abfangen von Daten zu vermeiden
- Beginn der Umsetzung eines Null-Vertrauens-Programms
- Denken Sie daran, die Privatsphäre der Endnutzer*innen zu respektieren

Über diese Studie:

Wir wollten die größten Sicherheitstrends am modernen Arbeitsplatz besser verstehen, einschließlich der Geräte, Benutzer*innen und Apps, die alle miteinander verbunden sein müssen, um die Arbeit zu erledigen. Die in diesem Dokument enthaltenen Informationen und Statistiken sind das Ergebnis unserer Analyse von Sicherheitstrends innerhalb unseres Kundenstamms sowie unserer eigenen Untersuchung von Betriebssystem- und Anwendungsschwachstellen und einer Studie über den bösartigen Untergrund. Um die realen Auswirkungen dieser Sicherheitstrends zu verstehen, haben wir über einen Zeitraum von 12 Monaten eine Stichprobe von 15 Millionen durch Jamf geschützten Geräten aus 90 Ländern untersucht, die sich auf iOS, macOS, iPadOS, Android und Windows beziehen. Diese Analyse wurde im vierten Quartal 2023 durchgeführt. Die in dieser Untersuchung analysierten Metadaten stammen aus zusammengefassten Protokollen, die keine persönlichen oder organisationsbezogenen Informationen enthalten. Mit dieser Analyse wollen wir keine Ängste schüren, sondern Sie und Ihre Benutzer*innen über die verfügbaren Optionen aufklären und darüber, wie Sie alle Aspekte der Geräte-, Benutzer*innen- und Unternehmensdaten am besten schützen können. Setzen Sie sich mit uns in Verbindung, um zu erfahren, wie Sie Schutzmaßnahmen ergreifen und Ihre Sicherheitslage verbessern können.

Quelle: Jamf Threat Labs