jamf

Sicherheit 360:

Jährlicher Trendbericht für Mobilgeräte

Einleitung

Über alle Branchen und Anwendungsfälle hinweg - von Workflows im Einzelhandel bis hin zu Abläufen im Gesundheitswesen - setzen Führungskräfte Innovationen für Mobilgeräte ein, um die Arbeitsweise der Mitarbeiter:innen zu verändern und die Unternehmensergebnisse zu optimieren. Für viele Mitarbeiter:innen in allen Branchen sind Mobilgeräte (z. B. Smartphones und Tablets) die einzigen Geräte, die am Arbeitsplatz verwendet werden. Und im modernen Arbeitsumfeld geht es darum, Mitarbeiter:innen die Möglichkeit zu geben, sich von überall, zu jeder Zeit und mit einem Gerät ihrer Wahl zu verbinden.

Einer der wichtigsten Treiber für mobiles Arbeiten war die Einführung von Mobilität als Service am Arbeitsplatz. Sie sind nicht mehr nur Begleitgeräte, sondern werden zunehmend zum wichtigsten Mittel, um die Arbeit zu erledigen. Mobilität ist zwar kein Fremdwort am Arbeitsplatz, aber ihre kontinuierliche Integration in wichtige Workflows ist ausgeprägter als je zuvor. Der Arbeitsplatz von heute erfordert nicht nur außergewöhnliche digitale Erlebnisse, sondern auch **sichere** digitale Erlebnisse, die die Produktivität der Arbeiter:innen maximieren, unabhängig davon, wo sie arbeiten.

- **Josh Stein,**
VP of Product Management

Einführung

Der Bericht „Sicherheit 360“ von Jamf basiert auf der Analyse realer Kundenvorfälle, Bedrohungsanalysen und Branchenereignissen des vergangenen Jahres. Dieser Bericht konzentriert sich auf die Untersuchung der Bedrohungslage im Mobilbereich, um die Risiken, denen Unternehmen ausgesetzt sind, zu beleuchten.

Wir bieten eine Bewertung der verschiedenen Angriffsvektoren, die aktiv eingesetzt werden, um Benutzer:innen auszutricksen, Mobilgeräte zu kompromittieren und Organisationen zu infiltrieren. Diese Angriffe beschränken sich nicht nur auf Schwachstellen auf Geräten. Unsere Analyse umfasst auch riskante Apps, Bedrohungen aus dem Internet und mehr.

Neben der Analyse dieser Bedrohungstrends enthält der Bericht auch eine Stellungnahme des CISO von Jamf, um Führungskräften, die ihre Mobilflotten auf Benutzer-, Geräte-, Anwendungs- und Netzwerkebene schützen wollen, einen umfassenden Einblick zu geben.

Methodik der Forschung

Um die tatsächlichen Auswirkungen der in diesem Bericht identifizierten Sicherheitstrends zu verstehen und zu quantifizieren, haben wir eine Stichprobe von 1,4 Millionen Geräten untersucht, die durch Jamf geschützt sind. Unsere Analyse wurde im ersten Quartal 2025 durchgeführt, wobei wir den vorangegangenen 12-Monats-Zeitraum überprüften und weltweit 90 Länder und mehrere Plattformen - insbesondere iOS, iPadOS und Android-Geräte - abdeckten.

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

Zweck der Forschung

Mit dieser Analyse wollen wir Organisationen und Benutzer:innen in die Lage versetzen, die aktuellen Trends im Bereich der Cybersicherheit besser zu verstehen, und aufzeigen, wie Organisationen und Benutzer:innen Maßnahmen zur Risikominderung ergreifen können. Er bietet außerdem eine Übersicht über die wichtigsten Untersuchungen von Jamf Threat Labs, einschließlich der gefundenen Bedrohungen und Schwachstellen. Indem wir unser Netzwerk über die aktuellen Entwicklungen informieren, hoffen wir, alle Mythen zu widerlegen und aufzuzeigen, wie Sie Schutzmaßnahmen zum Schutz Ihrer Nutzer:innen und Daten umsetzen können. Einige der häufigsten Best Practices, die Organisationen anwenden können:

- Kontinuierliche und zeitnahe Betriebssystem-Updates
- Nutzerschulung und -ausbildung
- Antragsprüfung
- Multi-Faktor-Authentifizierung
- Zero-Trust-Sicherheitsrahmenwerke
- Erstellung und Verwaltung von Compliance-Baselines
- Umsetzung von Richtlinien zur akzeptablen Nutzung von Unternehmensdaten

Wir haben unsere Analyse und den Bericht in vier Kategorien unterteilt, die unserer Meinung nach für Organisationen auf der ganzen Welt die höchste Priorität haben:

I. Phishing auf Mobilgeräten

II. Schwachstellenverwaltung

III. App-Risiken

IV. Malware & Spyware

Die Analyse in diesem Bericht stützt sich auf die Threat Intelligence von Jamf, eine umfassende Sammlung von Erkenntnissen, die aus originärer Bedrohungsforschung, realen Nutzungsmetriken sowie Nachrichtenanalysen und Datenfeeds gewonnen werden. Die Threat Intelligence von Jamf basiert auf manuellen Recherchen der Jamf Threat Labs und Data Science-Teams, die Geräte, Apps und den Netzwerkverkehr auf Risiken, Bedrohungen und Zero-Day-Schwachstellen überwachen.

Die Statistiken in diesem Bericht beziehen sich auf **Apple-** und **Android-Geräte**.

Wir haben auch einen Bericht zur Sicherheit 360, der sich auf **Mac Geräte** konzentriert und den Sie **hier** finden können.

Wichtige Trends für die Mobilität

I. Phishing bleibt eine Herausforderung für Unternehmen

Phishing ist nach wie vor eine weit verbreitete Angriffstechnik von Cyberkriminellen und sein Einfluss auf die Bedrohungslandschaft ist nach wie vor ungebrochen. Im September 2024 **veröffentlichte Apple einen Blog-Beitrag** mit einer Anleitung für iOS Nutzer:innen, um „Betrug zu vermeiden und zu erfahren, was zu tun ist, wenn Sie verdächtige E-Mails, Telefonanrufe oder andere Nachrichten erhalten". Unabhängig davon, wie sicher eine Plattform oder ein Betriebssystem auch sein mag, Social-Engineering-Techniken – wie Phishing – zielen darauf ab, Unternehmensdaten zu infiltrieren, indem sie bei dem am wenigsten sicheren Teil des Geräts ansetzen: dem Nutzer.

II. Eine einzige Schwachstelle kann Cyberkriminellen systemweiten Zugang verschaffen

Es stimmt, dass Schwachstellen in Software (sowohl OS als auch Apps) auftreten, die wir täglich nutzen. In der **NIST Special Publication 800-124rd** heißt es: „Bei typischer Software treten Fehler und Schwachstellen mit einer geschätzten Häufigkeit von ~25 Fehlern pro 1000 Zeilen Code auf." Allgemeine Schwachstellen und Gefährdungen (CVE), die in der National Vulnerability Database (NVD) veröffentlicht werden, geben der Öffentlichkeit einen Überblick über die CVEs, die im Umlauf sind. Diese Updates sind unerlässlich, aber der Patch muss erst installiert werden, bevor sie für das Unternehmen von Nutzen sein können.

Apple und Google liefern wichtige Informationen, wenn eine Schwachstelle entdeckt wird - und welches Update die Schwachstelle behebt. Beispielsweise hat Apple Anfang dieses Jahres iOS 18.3.2 als Reaktion auf **CVE-2025-24201 veröffentlicht** – dabei handelt es sich um eine Sicherheitslücke, durch die böswillig manipulierte Webinhalte aus der Sandbox für Webinhalte ausbrechen können. **Google hat das Android Security Bulletin veröffentlicht**, das 43 Sicherheitsschwachstellen behebt - darunter zwei kritische Zero-Day-Schwachstellen.

III. Apps bergen Risiken - selbst auf sicheren Plattformen

Seit seinem Debüt haben der App Store von Apple und der Google Play Store Nutzer:innen und Organisationen gleichermaßen geschützt. Apple Nutzer:innen sind beim Download und der Nutzung einer App aus dem App Store geschützt, da Apple „**jede App auf Malware und andere Software überprüft, die die Sicherheit und den Datenschutz der Nutzer:innen beeinträchtigen könnte**". Für Nutzer:innen von Android gibt es im Google Play Store Google Play Protect. Das hält die Bedrohungsakteure jedoch nicht auf. In den letzten fünf Jahren hat Apple über 9 Milliarden Dollar an potenziell betrügerischen Transaktionen verhindert.Der **Digital Markets Act der Europäischen Union** (DMA) ermöglicht die Einrichtung alternativer App-Marktplätze und verpflichtet „Gatekeeper" dazu, ihre geschlossenen Plattformen zu öffnen. Apps, die über alternative App Stores vertrieben werden, unterliegen nicht denselben Richtlinien wie die Apps aus dem App Store von Apple, was zu Risiken für die Sicherheit und den Datenschutz der Nutzer:innen führen kann. Social Engineering (z. B. Phishing), Ransomware, Spyware für Verbraucher und mehr sind als Risiken dokumentiert, die für Nutzer:innen entstehen können, die Apps herunterladen oder alternative Zahlungssysteme außerhalb des Apple App Store verwenden.

Für Android-Geräte **warnte Google Anfang des Jahres vor einem neuen Trojaner** , der „mehr als 750 legitime Banking- und Shopping-Apps angreift". Nun wurden die beiden gängigsten App-Stores gezwungen, Nutzer:innen in der EU das Sideloading von Apps zu ermöglichen, wodurch sich die Angriffsfläche für Bedrohungsakteure vergrößert hat.

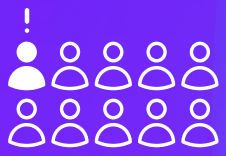
IV. Gezielte Angriffe gefährden Mobilgeräte

Mobilgeräte bieten die Flexibilität, dort zu arbeiten, wo wir wollen oder müssen; oft nutzen Führungskräfte Mobilgeräte, um weltweit Geschäfte zu tätigen. **Führungskräfte sind jedoch** aufgrund der auf ihren Geräten gespeicherten Daten - geistiges Eigentum, Finanzdaten und mehr - oft die am stärksten gefährdete Personengruppe. Angreifer:innen haben es auf gut vernetzte Führungskräfte abgesehen, die für ihre Erpressungsversuche am besten geeignet sind.

In den vergangenen zwölf Monaten haben wir folgendes gefunden:

25 %

der Unternehmen waren von einem Social-Engineering-Angriff betroffen



1 von 10

Nutzernhat auf einen bösartigen Phishing-Link geklickt

I. Phishing auf Mobilgeräten

Phishing ist eine der häufigsten und schädlichsten Bedrohungen, denen Organisationen heute ausgesetzt sind. Laut der Agentur für Cybersicherheit und Infrastruktursicherheit **„beginnen mehr als 90 % der erfolgreichen Cyberangriffe mit einer Phishing-E-Mail.**“

Phishing erfolgt über eine Vielzahl von Kanälen auf Mobilgeräten. Es geht nicht mehr nur um E-Mails: Die Angriffe erfolgen auch über SMS (Smishing genannt), soziale Medien oder Links zu gefälschten Websites.

Aber warum ist Phishing auf Mobilgeräten so viel erfolgreicher?

Zunächst ist es wichtig zu verstehen, dass **weltweit über 62 % der Webseitenaufrufe** von Mobilgeräten stammen. Dies bedeutet, dass mobile Geräte einen größeren Anteil am Internetverkehr ausmachen und Bedrohungsakteuren somit ein größeres Reservoir potenzieller Ziele zur Verfügung steht, die sie auf Schwachstellen untersuchen können.

Im Gegensatz dazu sind Mobilgeräte kompakte Geräte mit kleineren Bildschirmen. Das ist Teil ihrer Beliebtheit – dank ihrer Größe können die Nutzer:innen sie überallhin mitnehmen. Es ermöglicht Unternehmen auch die Implementierung von Arbeitsabläufen, die mobile Geräte einbeziehen, wie beispielsweise im:

- Einzelhandel (Point-of-Sale oder Bestand)
- Gesundheitswesen (Visite oder am Krankenbett)
- Produktion (Bediener-/Maschinenanweisungen)
- Luftfahrt (elektronische Flugtaschen oder Vorrichtungen unter den Tragflächen)

Doch gerade diese Vorteile machen es möglich, dass die Nutzer:innen bei bösartigen Phishing-Angriffen abgelenkt werden. Der Eindruck, dass mobile Geräte von Natur aus sicher sind, hält sich hartnäckig, aber wie wir dokumentiert haben, reicht ein einziger Link, um ein Gerät zu kompromittieren.

Die 20 häufigsten Marken, die in Phishing-Kampagnen verwendet werden

Mithilfe mobiler Geräte können Unternehmen neue Arbeitsabläufe implementieren, die Beziehung zu Kunden optimieren und das Nutzererlebnis verbessern. Die Nutzung mobiler Geräte ist heute für viele von uns selbstverständlich – sei es als Begleitgerät oder als wichtigstes Arbeitsmittel. Mobilgeräte verbinden uns mit unserem Leben - sowohl bei der Arbeit als auch in der Freizeit. Cyberkriminelle wissen das und nutzen es für ihre bösartigen Aktivitäten.

In unserer Untersuchung haben wir festgestellt, dass bestimmte beliebte Marken im Rahmen von Social-Engineering-Angriffen genutzt werden, um Endnutzer auf Mobilgeräten zu schädigen. Wir haben diese Marken in **vier Kategorien** unterteilt, die am häufigsten verwendet werden, um das Vertrauen der Nutzer:innen auszunutzen:

Die unzähligen Gründe für die Nutzung mobiler Geräte - Zugriff auf E-Mails bei der Arbeit, Bestellung von Haushaltsartikeln, persönliche Bankgeschäfte - haben dazu geführt, dass Bedrohungsakteure diese häufigen, oft notwendigen Anwendungsfälle ausnutzen, um Zugang zu Daten zu erhalten. In der nachstehenden Tabelle sind die zwanzig wichtigsten Marken aufgeführt, die beim Social Engineering verwendet wurden, basierend auf diesen vier Kategorien.

1.	2.	3.	4.
Unterhaltung	**Business**	**Dienstprogramme**	**Privat**
Netflix	Outlook	United States Postal Service (US-Postdienst)	Amazon.com Inc
Bet365	Office365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Facebook, Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Aufgrund ihrer Beliebtheit, ihres Ansehens und ihres Einflusses auf Unternehmen und Privatpersonen werden diese Marken häufig von Bedrohungsakteuren für Social Engineering-Angriffe ausgenutzt. Aufgrund ihres vertrauenswürdigen Rufs ist es wahrscheinlicher, dass Nutzer:innen auf schädliche Inhalte reagieren, die als legitime Kommunikation getarnt sind.

Diese Liste zeigt die 20 wichtigsten Marken, die im vergangenen Jahr ins Visier genommen wurden, ist aber bei weitem nicht erschöpfend. Cyberkriminelle passen sich ständig an, und die Marken, die sie nachahmen, können variieren. Letztendlich unterstreicht dies, wie Cyberkriminelle das Vertrauen, das diese Marken im Laufe der Jahre aufgebaut haben, ausnutzen, um Nutzer:innen zu täuschen und auszubeuten.

In der moderen Welt sind unsere personenbezogenen Daten ständig gefährdet. Da immer mehr Mobilgeräte sowohl für private als auch für berufliche Zwecke genutzt werden, wird der Aktionsradius der Angreifer:innen immer größer. Die Angreifer:innen wenden immer raffiniertere Taktiken an und nutzen realistische Benutzeroberflächen, Nutzererfahrungen und authentische Kommunikationsstile, um ahnungslose Opfer in ihre Falle zu locken. Es gibt jedoch Schutzmaßnahmen (z. B. kontinuierliche Mitarbeiterschulungen und Tools zur Bedrohungsprävention), die Unternehmen einsetzen können, um ihre Nutzer:innen und Daten zu schützen.

Jamf hat in einem **Zeitraum von 12 Monaten** etwa **10 Millionen Phishing-Angriffe** identifiziert, wobei **1,4 Millionen Geräte** unserer Stichprobe betroffen waren.

Darüber hinaus stellten wir fest, dass **1,5-2 %** dieser Angriffe regelmäßig als **Zero-Day** eingestuft wurden, was bedeutet, dass die Angreifer:innen brandneue, noch nie dagewesene Ziele verwenden, um Nutzer:innen dazu zu verleiten, auf bösartige Links zu klicken.

Das Erkennen und Überprüfen von Zero-Day Phishing-Angriffen hilft Organisationen, Nutzer:innen davor zu schützen, Opfer von brandneuen und unentdeckten Phishing-Seiten zu werden.

Aus der Perspektive des CISO

- **Einführung eines umfangreichen Schulungsprogramms:** Das war entscheidend für unseren Erfolg. Wir führen anspruchsvolle Phishing-Kampagnen und spielerische Schulungen durch, bieten einmalige Schulungen für Nutzer:innen an, die diese anfordern, und geben unseren Nutzer:innen die Möglichkeit, Phishing-E-Mails zu melden und gleichzeitig das ganze Jahr über Bestätigungen und Feedback zu ihren Einsendungen zu erhalten. Für uns ist dies nicht nur eine einmal im Jahr stattfindende Schulung, die dann „abgehakt" ist.
- **Halten Sie sich über neue Trends und Taktiken auf dem Laufenden:** Dies mag offensichtlich erscheinen, aber Cyberkriminelle nutzen immer alles aus, was sie können, und dazu gehört oft etwas Neues, Bahnbrechendes oder Kontroverses in den Nachrichten. Sie müssen Ihr Training und Ihre Blocking-Taktiken anpassen, um diese Herausforderungen zu meistern. Dies kann bei den Nutzer:innen zu einer gewissen Verunsicherung führen, aber Transparenz ist entscheidend. Die Schulung soll sie auf potenzielle Kriminelle vorbereiten, die keine Rücksicht auf ihre Gefühle nehmen, wenn sie Schaden anrichten, und oft sogar versuchen, eine emotionale Reaktion hervorzurufen, um das Opfer zu verwirren und zu überlisten.
- **Verfolgen Sie einen mehrschichtigen Ansatz:** Es gibt keine Einzellösung oder ein einziges Tool, um zu verhindern, dass Sie Opfer einer gezielten Phishing-Kampagne werden. Stellen Sie sicher, dass Sie aus mehreren Gesichtspunkten abgesichert sind. Blockieren Sie bösartige Domains. Implementieren Sie MFA. Nutzen Sie Zero-Trust. Die Regeln für unmögliche Geschwindigkeiten sind aktiviert. Aktivieren Sie die Regeln für unmögliche Geschwindigkeiten.

II. Management von Schwachstellen

Schwachstellen treten auf, wenn ein System, eine App oder ein Protokoll eine Lücke oder einen Fehler aufweist, der von Angreifer:innen ausgenutzt werden kann, um die Sicherheit, Integrität und/oder Verfügbarkeit des Systems zu gefährden. **Apple** und **Google** stellen eine Liste bekannter Schwachstellen zur Verfügung, die ihre Betriebssysteme betreffen. Das bedeutet jedoch, dass es diese Schwachstellen gibt, bevor Apple oder Google ein Update und einen Sicherheitspatch bereitstellen. Vom 1. Januar 2024 bis zum 1. April 2025 dokumentierte Apple **29 Sicherheitsupdates** mit zugehörigen CVEs für Haupt- und Nebenversionen von iOS. Im gleichen Zeitraum dokumentierte Android im Android Security Bulletin **39 Systemschwachstellen** mit zugehörigen CVEs.

Apple (über **Schnelle Sicherheitsreaktionen**) und Google (über **Android-Sicherheitspatches**) geben zwischen den Software-Updates eigenständige Sicherheitspatches heraus. Warum sind diese Patches von Vorteil? Es handelt sich um zeitnahe Updates, d. h. Organisationen können Updates automatisch insallieren, ohne auf größere Updates warten zu müssen.

Moderne **Cyberbedrohungen** sind kreativ und komplex, und sowohl die Verbraucher:innen als auch Unternehmen müssen bei der Aktualisierung von Geräten wachsam sein. Es geht nicht nur darum, das Gerät zu aktualisieren, sondern auch zu überprüfen, ob das **Update authenthisch** ist.

Jamf Threat Labs hat sich vor kurzem mit einer bestimmten Methode beschäftigt, die während einer Angriffssequenz verwendet wird - der Aufrechterhaltung der Persistenz. Ihre Untersuchungen zeigten, wie „Angreifer die iOS-Einstellungsoberfläche ausnutzen und die Systemaktualisierungseinstellungen manipulieren könnten, einschließlich Aufforderungen und Benachrichtigungen, die auf eine verfügbare Aktualisierung von iOS hinweisen.“

Werfen wir einen genaueren Blick auf einige bemerkenswerte Schwachstellen aus den jüngsten Veröffentlichungen von Apple: (dieser Bericht wurde im April 2025 verfasst)

Behebung von CVEs bei Apple	Datum	Einstufung der Schwachstellen	Auswirkungen
iOS 18.4.1 und iPadOS 18.4.1	April 2025	CVE-2025-31200 CVSS - Score: 7,5 | Schweregrad: hoch	CoreAudio
iOS 18.4 und iPadOS 18.4	April 2025	CVE-2025-30430 CVSS - Score: 9,.8 | Schweregrad: kritisch	Authentifizierungsdienste
iOS 18.3 und iPadOS 18.3	Januar 2025	CVE-2025-24085 CVSS – Score: 7,8 | Schweregrad: hoch	CoreMedia
iOS 18.3 und iPadOS 18.3	Januar 2025	CVE-2025-24154 CVSS - Score: 9,1 | Schweregrad: kritisch	WebContentFilter

Aktualisierte AOSP*-Versionen	Datum	Einstufung der Schwachstellen	Auswirkungen
13, 14, 15	April 2025	CVE-2025-26416 Schweregrad: kritisch	Erweiterung der Berechtigungen
15.	März 2025	CVE-2025-22403 Schweregrad: kritisch	Code-Ausführung aus der Ferne
15.	Februar 2025	CVE-2025-0096 Schweregrad: hoch	Erweiterung der Berechtigungen
12, 12L, 13, 14, 15	Januar 2025	CVE-2024-43771 Schweregrad: kritisch	Code-Ausführung aus der Ferne

*Android Open Source-Projekt

Die Schwachstellen - alle auf der Website von Apple und Android aufgelistet - zeigen uns, dass bei der Entwicklung von Software Schwachstellen auftreten können. Für Sicherheitsexperten ist es wichtig, dass sie diese Schwachstellen erkennen und Maßnahmen ergreifen können, um ihre Daten zu schützen.

Eine der besten Möglichkeiten, dies zu erreichen, sind aktuelle Betriebssysteme - und die Tools, um diese Updates zu installieren.

Aufrechterhaltung eines guten Sicherheitsstatus mit aktualisierten Betriebssystemen

Die beste Möglichkeit für Unternehmen, Schwachstellen zu beseitigen und ihre Organisation konform zu halten, ist ein Update des Betriebssystems ihrer Geräte. Wie auf der vorherigen Seite gezeigt, stellen sowohl Apple als auch Android regelmäßig Updates für OS mit bekannten Schwachstellen bereit.

Eine gängige Methode für Unternehmen, das OS (und die Apps, die ihre Mitarbeiter:innen täglich nutzen) zu aktualisieren, ist eine Mobile Device Management (MDM)-Lösung. MDM bietet auch ausführliche Berichte für das Betriebssystem, das auf jedem verwalteten Gerät installiert ist. In Unternehmen gibt es jedoch häufig viele Geräte, die für unterschiedliche Anwendungsfälle genutzt werden und auf denen verschiedene Apps für unterschiedliche Nutzer:innen laufen. Es ist schwierig (und oft nicht machbar - z. B. das Testen von Apps vor der Bereitstellung), jedes Gerät in einer Flotte mit dem aktuellsten Betriebssystem auszustatten.

In den letzten zwölf Monaten:

32 %

der Organisationen betreiben mindestens ein Gerät mit kritischen (und patchbaren) Schwachstellen

55,1 %

deram Arbeitsplatz verwendeten Mobilgeräte verfügen über ein anfälliges Betriebssystem

Es wurde festgestellt, dass Organisationen Mobilgeräte ohne die neuesten Sicherheitspatches betreiben. Unseren Daten zufolge wurden **4,8 %** aller Android-Geräte mit Sicherheitslücken für den Zugriff auf Unternehmensressourcen verwendet.

Mobilität lässt uns arbeiten, wie wir wollen. Von der Entgegennahme von Geschäftsgesprächen im Auto bis hin zur Erweiterung von Workflows für Mitarbeiter:innen im Außendienst und mit Kundenkontakt – mobile Geräte eröffnen neue Möglichkeiten am Arbeitsplatz. Aber wie jedes andere Gerät ist auch dieses System anfällig für Bedrohungen. Unternehmen können Maßnahmen ergreifen, um Bedrohungen für ihre Mobilgeräte durch Tools zu verringern, die ein Gleichgewicht zwischen Benutzerfreundlichkeit und Sicherheit herstellen, Mitarbeiter:innen schulen und ein Verständnis für die heutzutage am häufigsten auftretenden Bedrohungen vermitteln.

Aus der Perspektive des CISO

- **Sorgen Sie für Sichtbarkeit der Schwachstellen in Ihrer gesamten Organisation:**
  Ein guter Ausgangspunkt ist es, sich einen Überblick über die Schwachstellen auf Ihren Geräten oder in Ihrer Infrastruktur zu verschaffen. Sie können mit diesen Daten beginnen, um den Fußabdruck einer bestimmten Anwendung, potenzielle Risiken, den Wirkungsradius usw. zu analysieren. Auf diese Weise können Sie Ihre Schwachstellen auf der Grundlage von Daten nach Prioritäten ordnen.
- **Führen Sie ein solides Patching-Programm ein:**
  Um auf den Punkt MDM zurückzukommen: Ein Tool, das sicherstellt, dass Sie mit den neuesten oder unterstützten N -X-Versionen von Software oder OS Schritt halten können, ist für eine stabile und sichere Umgebung von größter Bedeutung. Wenn dies mit geringen oder gar keinen Auswirkungen auf die Endbenutzer:innen geschieht, ist es einfacher, Partnerschaften einzugehen und das Unternehmen zu unterstützen.
- **Implementieren Sie einen risikobasierten Zugangsansatz:**
  Wenn nicht konforme Geräte versuchen, auf die Ressourcen Ihres Unternehmens zuzugreifen, sollten Sie diesen Zugang blockieren, bis die Nutzer:innen entsprechende Maßnahmen ergreifen, um das Gerät mit möglichst geringem Aufwand wieder konform zu machen.

III. App-Risiko

Ende November 2024 veröffentlichte die Agentur für Cybersicherheit **einen Bericht über die am häufigsten ausgenutzten Schwachstellen im Jahr 2023**. (Dies ist die neueste Version des Berichts.) Der Bericht befasst sich eingehend mit den 15 wichtigsten Schwachstellen - einschließlich Details darüber, was die Angreifer:innen mit der Schwachstelle anrichten können. Die Schwachstellen befinden sich in Betriebssystemen auf verschiedenen Computer-Plattformen und in Anwendungen, die die Mitarbeiter:innen und Schüler:innen einer Organisation täglich nutzen. In dem Bericht heißt es: „Böswillige Cyberkriminelle nutzten im Jahr 2023 mehr Zero-Day-Schwachstellen aus, um Unternehmensnetzwerke zu kompromittieren, als im Jahr 2022, wodurch sie Angriffe auf Ziele mit hoher Priorität durchführen konnten." Die Agentur für Cybersicherheit beschreibt zudem, was Entwickler:innen und Nutzer:innen tun können, um Schwachstellen zu entschärfen. Für Endbenutzerorganisationen nennt der Bericht:

- *Zeitnahe* Aktualisierung von Software, OS, Apps und Firmware
- Routinemäßige Durchführung einer automatischen Bestandsermittlung
- Implementierung eines robusten Patch-Management-Prozesses
- Dokumentation sicherer Basiskonfigurationen
- Regelmäßige Durchführung sicherer System-Backups
- Erstellung eines aktualisierten Plans zur Reaktion auf Cybersicherheitsvorfälle

Was macht eine App „riskant"? Zu den wichtigsten Eigenschaften riskanter Apps gehören:

- Anomale Merkmale
- Bösartige Codemuster
- Gefährliche Genehmigungen
- Riskantes, dynamisches Verhalten
- Verdächtige Entwicklerprofile

Durch die Einsicht in App-Versionen, etwaige undichte Apps und mehr behalten Unternehmen die Nase vorn und sind bereit, das Risiko sofort zu untersuchen und zu beheben.

Für Unternehmen ist es wichtig, den Zustand ihrer Apps genau zu kennen. Einige der wichtigsten Datenpunkte, auf die Organisationen achten sollten, um riskante Apps zu erkennen und das Problem zu beheben, sind:

- Anzahl der Nutzer:innen, die eine veraltete App installiert haben
- Anzahl der Nutzer:innen mit einer bestimmten App-Version
- Liste der Apps mit fehlerhaften Verschlüsselungsimplementierungen, wodurch sensible Daten in ungeschützte Netzwerke gelangen können
- Apps, die bestimmte Berechtigungen anfordern, um Zugang zu Daten auf anderen Teilen des Geräts zu erhalten

Ein eingehender Blick auf eine reale Schwachstelle
Umgehung von Transparenz, Zustimmung und Kontrolle (TCC)

In allen Apple Betriebssystemen dient TCC als wichtiges Security Framework, das die Nutzer:innen dazu auffordert, Anfragen einzelner Apps nach Zugang zu sensiblen Daten wie Fotos, Kontakten und Standortangaben zu genehmigen oder abzulehnen. Eine TCC-Umgehungsschwachstelle tritt auf, wenn diese Kontrolle versagt, sodass eine Anwendung ohne die Zustimmung oder das Wissen der Nutzer:innen auf private Informationen zugreifen kann. Das bedeutet, dass die Angreifer:innen unbefugten Zugang zu Dateien und Ordnern, Gesundheitsdaten, dem Mikrofon oder der Kamera und mehr erhalten können, ohne dass Nutzer:innen gewarnt werden.

Jamf Threat Labs hat CVE-2024-44131 gefunden, eine TCC-Bypass-Schwachstelle, die File Provider auf iOS Geräten betrifft. Apple reagierte schnell auf diese Entdeckung mit einem Patch in iOS 18.0. CVEs wie CVE-2024-44131 sind wichtige Hinweise auf die Notwendigkeit, Geräte in Unternehmen auf dem neuesten Stand zu halten.

Schutz im App Store und Betrugsversuche

Wie bereits in diesem Bericht erwähnt, hat Apple in den letzten fünf Jahren betrügerische Transaktionen im Wert von über 9 Milliarden Dollar verhindert. Allein im Jahr 2024 hat das Unternehmen mehr als 2 Milliarden Dollar an betrügerischen Transaktionen blockiert. Im Jahr 2024 hat Apple:

- Mehr als 146.000 Accounts von Entwickler:innen wegen Betrugsverdachts gekündigt
- Weitere 139.000 Registrierungen von Entwickler:innen abgelehnt
- Über 43.000 Apps mit versteckten oder undokumentierten Funktionen abgelehnt
- Über 320.000 Einsendungen, die andere Apps kopierten, als Spam eingestuft, oder Nutzer:innen anderweitig in die Irre führten, abgelehnt.
- Mehr als 10.000 illegale, raubkopierte Apps identifiziert und blockiert

Der App Store gilt allgemein als die sicherste, benutzerfreundlichste und privateste Möglichkeit, Apps herunterzuladen. Der App Store für iOS verwendet Sandboxing, fragt die Nutzer:innen um Erlaubnis und lässt nur signierten Code auf dem Gerät laufen. Doch wie die Daten zeigen, gibt es nach wie vor bösartige Akteure und potenzielle Betrüger. Apples Engagement, den App Store zu einem sicheren, vertrauenswürdigen Ort für Apps zu machen, schützt Nutzer:innen und Entwickler:innen seit seiner Einführung im Jahr 2008. Für sogenannte „Sideloaded Apps“ - Apps aus Drittanbieter App Stores, wie AltStore - gilt dieser Schutz jedoch nicht.

Aus der Perspektive des CISO

Wirksame mobile Sicherheit erfordert einen mehrschichtigen Ansatz. Die Verwendung der neuesten Hardware eines vertrauenswürdigen Anbieters und des aktuellsten Betriebssystems reicht immer noch nicht aus, um Ihre Organisation und Ihre sensibelsten Assets vor Hacking zu schützen. Gute Sicherheitspraktiken müssen sich auf jede Ebene Ihres Tech-Stacks erstrecken , und das gilt auch für Apps.

- **Führen Sie für die sensiblen mobilen Apps Ihrer Organisation ein Programm zur Überprüfung von Apps ein:** Beginnen Sie mit den wichtigsten Apps und überprüfen Sie routinemäßig, ob in der gesamten Organisation die neuesten, sicheren Versionen ausgeführt werden. Überprüfen Sie bei der Skalierung des Programms jede App, die in den App Store Ihres Unternehmens aufgenommen wird.
- **Entwickeln Sie Richtlinien, die Geräte als „nicht mehr konform“ kennzeichnen**, wenn unerwünschte Apps installiert sind. Verhindern Sie, dass diese gefährdeten Geräte Zugang zu Ihren SaaS-Anwendungen, kritischen Rechenzentren oder Workloads aus der Ferne haben, bis die riskanten Apps aktualisiert oder entfernt wurden.
- **Integrieren Sie die Sicherheit mobiler Apps in Schulungen**, damit die Nutzer:innen Teil der Lösung werden können, indem sie bei Bedarf Updates auf Geräten durchführen, die sie im Arbeitsalltag bei sich haben.
- **Wenn Ihre Organisation keine alternativen App Marketplaces benötigt**, legen Sie Richtlinien fest, die den Zugang zu alternativen Stores auf Arbeitsgeräten verhindern. Verhindern Sie außerdem, dass Apps von der Seite geladen werden, um sicherzustellen, dass nur Apps aus offiziellen Quellen auf dem Gerät verwendet werden.

Das Team von Jamf Threat Labs veröffentlichte eine Demonstration, wie eine seitlich geladene App für Soziale Medien Fotos überwacht und auf den Server eines Angreifers hochlädt. Diese App wurde „modifiziert, aber funktioniert einwandfrei“. Das Team bietet einige klare Garantien zur Verbesserung der Sicherheit, nämlich:

- Aktivieren und regelmäßiges Überprüfen des App-Datenschutzberichts
- Seien Sie selektiv bei der Vergabe von Apps
- Vermeiden Sie die Speicherung von sensiblen Informationen

Laden Sie nur Apps aus zuverlässigen Quellen (wie dem App Store) herunter

Sowohl native Apps als auch in der Cloud gehostete Webanwendungen sind anfällig für Risiken. In der Cloud gehostete Apps sind aufgrund der größeren Angriffsfläche stärker gefährdet. Mit den richtigen Sichtbarkeits-, Kontroll- und Behebungsfunktionen können Organisationen jedoch risikoreiche Apps am Arbeitsplatz eindämmen.

IV. Gezielte Angriffe und anspruchsvolle Spyware

Seit 2021 **hat Apple** Bedrohungsmitteilungen an Nutzer:innen in über 150 Ländern verschickt. Diese Mitteilungen informieren und unterstützen Nutzer:innen, in der Regel wichtige Personen wie Journalist:innen, Politiker:innen oder Diplomat:innen, die Ziel von Angriffen durch Spyware sind. Und Ende April 2025 schickte Apple „diese Woche Benachrichtigungen an mehrere Personen, von denen das Unternehmen glaubt, dass sie mit Spionageprogrammen der Regierung infiziert wurden". Aber es betrifft nicht nur Apple. Diese Angriffe zielen auf alle Arten von Betriebssystemen und Apps ab. **Laut The Citizen Lab** wurde „Spyware in WhatsApp sowie in andere Apps auf ihren [Android-] Geräten geladen".

Malware und Spyware, wie sie Apple in Bedrohungsbenachrichtigungen meldet, gehören zu den fortschrittlichsten Bedrohungen, denen Unternehmen und Einzelpersonen heute ausgesetzt sind. Aber es gibt Schutzmaßnahmen, die alle Nutzer:innen - auf jeder Ebene Ihrer Organisation - vor diesen fortschrittlichen Bedrohungen schützen.

Apple bietet für alle Nutzer:innen Anleitungen zum Schutz vor Malware an, von denen wir viele bereits in diesem Artikel behandelt haben. Konkret rät Apple den Nutzer:innen zu folgenden Dingen:

- Aktualisieren Sie die Geräte auf die neueste Software, da diese die neuesten Sicherheitskorrekturen enthält.
- Schützen Sie Geräte mit einem Passwort.
- Verwenden Sie die Zwei-Faktor-Authentifizierung und ein sicheres Passwort für Ihren Apple Account.
- Installieren Sie Ihre Apps aus dem App Store.
- Verwenden Sie online sichere und individuelle Passwörter.
- Klicken Sie nicht auf Links oder Anhänge von unbekannten Absendern.

Jamf Threat Labs: Kompromittierung eines Geräts ohne das Wissen des Opfers

Jamf Threat Labs demonstrierte, wie ein Gerät - ohne schützende Software - ohne das Wissen des Opfers kompromittiert wurde. Die Demo zeigte, wie sich Cyberkriminelle Zugang zu E-Mail, Corporate Messaging, Zwei-Faktor-Authentifizierung und weiteren personenbezogenen Daten verschaffen können. Anschließend demonstriert das Team, wie Organisationen unternehmenseigene und personenbezogene Daten schützen können:

1. Erzwingen Sie sichere Konfigurationen, um die Compliance sowohl auf unternehmenseigenen als auch auf BYO-Geräten aufrechtzuerhalten
2. Aktivieren Sie Bedrohungsprävention und -überwachung mit gezielten Maßnahmen und schützen Sie dabei die Privatsphäre der Nutzer:innen
3. Erzwingen Sie die Geräteverschlüsselung auf allen verwalteten Geräten

Aus der Perspektive des CISO

Malware ist auf Mobilgeräten nicht so weit verbreitet wie auf anderen primären Computern. Wenn sie jedoch entdeckt werden, wird oft festgestellt, dass sie sehr fortgeschrittene Techniken verwenden und auf Einzelpersonen abzielen.

- **Werden Sie nicht zu nachlässig** und gehen Sie nicht davon aus, dass mobile Malware niemals Ihr Unternehmen betreffen wird. Erst im vergangenen Jahr hat Apple Nutzer:innen in rund 100 Ländern über die Gefährdung durch Spyware informiert.
- **Beauftragen Sie mindestens einen Verantwortlichen** für die mobile Sicherheit und stellen Sie ihm die Aufgabe, regelmäßig Berichte über den Zustand der mobilen Bereitstellung in Ihrem Unternehmen zu erstellen. Katalogisieren Sie Vorfälle von gestohlenen Telefonen, gezieltem Phishing, Leistungseinbrüchen und alles andere, was auf ein unregelmäßiges Verhalten hinweist. Idealerweise sollten Sie einen Telemetrie-Stream von Ihren Geräteverwaltungs- und Sicherheitstools einrichten und diese Daten in Ihr Security Operations Center einfließen lassen. Behandeln Sie Mobilgeräte wie jeden anderen Endpoint.
- **Sammeln Sie, wenn möglich, Daten über mobile Systeme und schauen Sie nach Hinweisen auf Zero-Day-Angriffe.** Hierfür ist Fachwissen erforderlich, das entweder in-house oder auf Vertragsbasis erworben werden kann. Investieren Sie bei Unternehmensorganisationen mit dedizierten Sicherheitsanalysten in die Entwicklung von Fachwissen zur mobilen Forensik in Ihren Teams.

Die wichtigsten Erkenntnisse

Mobiles Phishing ist eine der häufigsten Methoden für Cyberkriminelle, um sich Zugang zu sensiblen Daten zu verschaffen. Organisationen, die in der Lage sind, ein Schulungsprogramm zu implementieren, bei den neuesten Trends auf dem Laufenden zu bleiben (einschließlich der Anpassung von Schulungen) und einen mehrschichtigen Ansatz für die Sicherheit zu verfolgen, sind aus verschiedenen Perspektiven geschützt.

Schwachstellen treten in Software aller Art auf. Durch die Einführung einer angemessenen Sicherheitshygiene werden die Risiken gemindert, die durch Schwachstellen entstehen können. Regelmäßige Updates der Betriebssysteme und das Deaktivieren unnötiger Kontrollen (z. B. App Stores von Drittanbietern) helfen Organisationen dabei, die internen Grundregeln und externen Frameworks einzuhalten.

Eine unsachgemäße App-Verwaltung und -Nutzung birgt Risiken. Es ist nicht immer die App selbst, sondern auch andere Apps, die schädliche Netzwerkverbindungen herstellen. Durch die Einrichtung eines App-Stores für Unternehmen und die kontinuierliche Überprüfung von Apps (insbesondere für private und benutzerdefinierte Apps) können Organisationen anfällige Anwendungen besser überwachen, beheben und patchen.

APT- und Spyware-Angriffe kommen immer häufiger vor. Diese Bedrohungen (die oft von Nationalstaaten oder spezialisierten Gruppen ausgehen) betreffen Organisationen auf der ganzen Welt und zielen oft auf Führungskräfte ab, die vertrauliche Daten auf ihren Geräten haben. Mit einer umfassenden Sicherheitsstrategie, die Mobilgeräte wie jedes andere Gerät behandelt, können Organisationen Schutzmaßnahmen für das Ökosystem ihrer Mobilgeräte und die Daten, mit denen die Geräte verbunden sind, gewährleisten.

Erstellen und implementieren Sie Richtlinien zur akzeptablen Nutzung für unternehmenseigene Geräte, die durchsetzbare Richtlinien zur akzeptablen Nutzung erfordern, eine Verbindung zu Arbeitsressourcen herstellen oder organisatorische Richtlinien einhalten müssen. **Bei BYO-Geräten sind für diese Geräte zusätzliche Datenschutzkontrollen erforderlich, wie der Datenschutz, den Apple** für Geräte bietet.

jamf

Kontaktieren Sie uns, um mehr über die Bedrohungslage im Mobilbereich zu erfahren.