jamf

Sicherheit 360:

Jährlicher Trendbericht für

Mobilgeräte

Inhaltsverzeichnis:

Einführung

Jamfs Bericht „Sicherheit 360" bietet eine fundierte Retrospektive der sich ständig weiterentwickelnden Bedrohungslage; sie stützt sich auf reale Vorfälle innerhalb unseres Kundenstamms, neuartige Entdeckungen unserer Bedrohungsforscher sowie Beobachtungen aus globalen, nationalen und branchenspezifischen Ereignissen. Dieser Bericht konzentriert sich auf die Untersuchung der Bedrohungslage im Mobilbereich, um die Risiken, denen Unternehmen ausgesetzt sind, näher zu beleuchten.

Wir untersuchen die vielfältigen und folgenschweren Angriffsvektoren, die Angreifer nutzen, um sich Zugriff zu verschaffen, sich von einem System zum nächsten vorzuarbeiten und letztlich Daten zu kompromittieren oder Schaden anzurichten. Angreifer nutzen Schwachstellen von Geräten und Software aus, schleusen bösartigen Code in Apps und Web-Kommunikation ein und bedrohen Benutzer, das schwächste Glied in der Verteidigungskette eines jeden Unternehmens, um ihre Ziele zu erreichen.

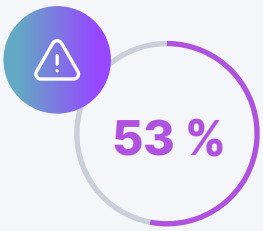
Zusätzlich zur Analyse dieser Bedrohungstrends enthält der Bericht eine Stellungnahme des CISO von Jamf. Er bietet damit wertvolle Einblicke für Sicherheitsverantwortliche und IT-Experten, die für den Schutz mobiler Flotten zuständig sind.

Methodik der Forschung

Um die realen Auswirkungen der in diesem Bericht identifizierten Sicherheitstrends zu verstehen und zu quantifizieren, haben wir eine Stichprobe aus über 1,7 Millionen iOS- und Android-Geräten innerhalb unseres Kundenstamms anonym untersucht. Unsere Analyse wurde Ende 2025 durchgeführt, wobei wir den vorangegangenen 12-Monats-Zeitraum überprüften und dabei weltweit mehrere Länder einbezogen.

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 Daten oder Informationen zur Identifizierung der Organisation enthalten.

Wichtigste Ergebnisse



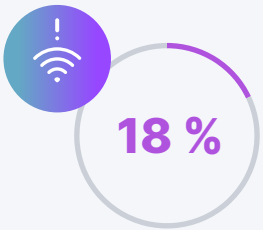
Der Anteil der Unternehmen, die mindestens ein Gerät mit einem veralteten Betriebssystem hatten

Ein veraltetes Betriebssystem bedeutet ungepatchte Schwachstellen, die ausgenutzt werden können. Das Automatisieren und Erzwingen von Updates trägt wesentlich zum Schutz Ihrer Geräte bei.

1 von 850

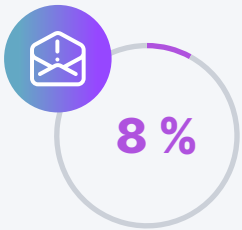
Die Anzahl der beruflich genutzten – und jailbroken – Geräte

Jamf erkannte diese Geräte; kontextbasierte Zugriffsrichtlinien verhinderten den Zugriff auf Unternehmensressourcen.



Der Anteil der Unternehmen mit Mitarbeitern, die sich mit riskanten Hotspots verbinden

Riskante Hotspots öffnen Tür und Tor für Infrastrukturbedrohungen wie betrügerische Zugangspunkte oder Adversary-in-the-Middle-Angriffe, vor allem, wenn die Geräte nicht so konfiguriert sind, dass sie diesem Risiko standhalten.



Der Anteil der Geräte, auf denen jemand auf einen Phishing-Link geklickt hat

Phishing-Angriffe sind nach wie vor eine beliebte Taktik von Angreifern, um Accounts zu kompromittieren, wobei sich daran im Vergleich zum Vorjahr kaum etwas geändert hat. Ohne entsprechende Schutzmaßnahmen können die Auswirkungen verheerend sein.

Zero-Clicks- und Browser-Angriffe

Nach wie vor beliebte und wirksame Methoden

Sowohl in Betriebssystemen als auch in Software tauchen weiterhin Sicherheitslücken auf; diese bieten Angreifern die Möglichkeit, mithilfe verschiedener Spyware-Familien an sensible Informationen zu gelangen. Dieser Bericht unterstreicht, wie wichtig es ist, die Risiken auf Ihren mobilen Geräten strategisch zu reduzieren.

Wichtige Trends in Unternehmen

Mobile Geräte helfen den Mitarbeitern, produktiv zu bleiben, wo auch immer sie arbeiten. Die Art und Weise, wie wir diese Geräte verwalten und nutzen, und die Bedrohungen, denen sie ausgesetzt sind, bestimmen, wie sie gesichert werden.

Ihr Unternehmen kämpft jeden Tag darum, die Angriffsfläche zu verringern. Sie implementieren Kontrollen und Richtlinien und bestücken Ihr technisches System mit der besten Sicherheitssoftware, doch auch die Angreifer entwickeln sich weiter und bleiben hartnäckig.

Es gibt viele Komponenten, die Ihre Angriffsfläche ausmachen. In diesem Bericht sprechen wir über die größten Risiken, die Unternehmen nur schwer kontrollieren können und die Angreifer häufig ausnutzen – und darüber, wie man katastrophale Folgen vermeiden kann.

1. Schwachstellen in Software und Geräten sind Teil des Geschäfts.

Trotz aller Sorgfalt, die in die Entwicklung der Betriebssysteme Ihrer mobilen Geräte fließt, ist Perfektion unmöglich. 2025 wurden mehr als 48.000 CVE-Einträge veröffentlicht. Das sind eine Menge Schwachstellen, die es zu erkennen und zu beseitigen gilt.

Aber die Entwickler wissen das, und deshalb veröffentlichen sie Sicherheitspatches. Hier kommen Ihre Teams ins Spiel. Setzen Sie diese Patches um? Halten Sie Ihre Betriebssysteme auf dem neuesten Stand? Befolgen Sie bewährte Sicherheitsverfahren? Die Art und Weise, wie Sie Ihre Geräte konfigurieren, ist entscheidend.

Angreifer nutzen Schwachstellen aus und die Angriffsfläche wächst.

2. Mobile Apps können ein Segen oder ein Fluch sein.

Apps sind ein wesentlicher Bestandteil der mobilen Arbeit. Wahrscheinlich stellt Ihr Unternehmen Dutzende - oder Hunderte - von Apps in seiner Flotte bereit. Jede App birgt ihre eigenen Risiken. Malware für Mobilgeräte ist relativ selten, aber Datenschutz, Lieferketten und der Umgang mit Daten sind nach wie vor potenzielle Gefahren.

Auch Ihre Aps müssen immer auf dem neuesten Stand sein, denn deren Entwickler patchen ebenfalls Schwachstellen. Die Verwaltung des Lebenszyklus einer App ist von entscheidender Bedeutung, ebenso wie die Gewährleistung eines ausgewogenen Verhältnisses zwischen Sicherheit und Datenschutz für Ihre Mitarbeiter.

Apps vervielfachen die potenziellen Risiken und die Angriffsfläche wächst.

3. Netzwerke und Internetrisiken bedrohen selbst die sichersten Geräte.

Und der Schutz Ihrer Daten steht auf dem Spiel, ob im Ruhezustand oder bei der Übertragung. Um dies zu erreichen, müssen Sie Ihre Netzwerkinfrastruktur und das Verhalten der Benutzer verstehen. Mitarbeiter verbinden sich häufig mit ungeschützten Hotspots, die für Adversary-in-the-Middle (AitM)-Angriffe anfällig sind. Ohne die richtige Konfiguration sind Ihre Daten ungeschützt.

Phishing und andere Internetrisiken sind nach wie vor weit verbreitet. Angreifer imitieren populäre Websites aus verschiedenen Online-Kategorien: Unterhaltung, Business, Hilfsprogramme und Finanzen. Und die Benutzer fallen jeden Tag darauf herein, zumal die generative KI den Angreifern hilft, ihre Techniken zu verbessern.

Benutzerfehler und externe Netzwerke bieten unkontrollierte Einstiegspunkte und die Angriffsfläche wächst.

4. Die Risiken vervielfachen sich und führen zu fortgeschrittenen Bedrohungen.

Sicherheitslücken in Geräten, Apps, der Netzwerkinfrastruktur und das Benutzerverhalten können allesamt Schwachstellen in Ihrem Cyber-Schutzschild verursachen. Je größer Ihre Angriffsfläche ist, desto schwieriger ist es, sie abzudecken, und diese drei Risikoarten werden häufig für gezielte Angriffe ausgenutzt.

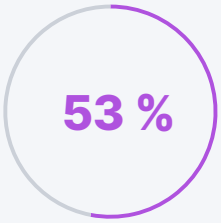
Die zunehmende Verbreitung dieser Gefahren kann Tür und Tor für schädlichere Angriffe, wie Advanced Persistent Threats (APT) und Spyware, öffnen. 2025 beobachtete Jamf Threat Labs eine fortgesetzte Ausnutzung von Systemen durch Zero-Click- und One-Click-Angriffe. Besonders betroffen waren Führungskräfte, Politiker, Aktivisten und Journalisten.

Wir haben einige der heimtückischsten Zero-Click- und One-Click-Angriffe im Jahr 2025 untersucht. Diese Angriffe zielen darauf ab, sensible Geheimdienstinformationen zu entwenden und verschiedene Komponenten eines Geräts auszunutzen. Im weiteren Verlauf dieses Berichts werden wir unsere Ergebnisse näher erläutern.

Schwachstellen von Geräten

Betriebssysteme für Mobilgeräte bieten eine Grundlage – sicher oder nicht.

Die Codebasis des Betriebssystems Ihres Geräts ist riesig und komplex. Und da Menschen fehlbar sind, wird es unweigerlich zu Schwachstellen im Code kommen. Und die Menschen sind schlau: Angreifer sind immer auf der Suche nach potenziellen Schwachstellen.



der **Unternehmen** haben mindestens ein Gerät mit einem veralteten Betriebssystem

Was ist ein CVE?

Das Programm „Allgemeine Schwachstellen und Gefährdungen" (CVE) dient als Datenbank für Schwachstellen, die von der Cybersicherheits-Community entdeckt wurden. Jede CVE-Liste identifiziert die betroffene Software oder Bibliothek, listet einen Schweregrad auf und beschreibt mögliche Methoden zur Ausnutzung.

Sehen wir uns einige prominente Beispiele aus dem Jahr 2025 an, von denen bestätigt wurde, dass sie unter realen Bedingungen ausgenutzt wurden. Diese CVEs wurden in iOS 18.4.1 gepatcht.

CVE-2025-31200

Schweregrad: 9,8 (kritisch)

Die Verarbeitung eines Audiostreams in einer böswillig gestalteten Mediendatei kann zur Ausführung von Code führen.

CVE-2025-31201

Schweregrad: 9,8 (kritisch)

Ein Angreifer mit beliebigen Lese- und Schreibfähigkeiten kann möglicherweise die Pointer-Authentifizierung umgehen.

Angreifer können Schwachstellen wie diese ausnutzen, um Ihre Daten auszuspähen und Spyware bereitzustellen. Stellen Sie sich folgendes (stark vereinfachtes) Szenario vor:

1. Eine hochrangige Zielperson erhält eine sorgfältig ausgearbeitete Nachricht, die eine schädliche Audiodatei enthält.
2. Das Mobilgerät verarbeitet die Audionachricht zur Vorschau ohne menschliche Interaktion.
3. Die Beschädigung des Speichers während der Verarbeitung ermöglicht beliebige Lese- und Schreibfunktionen.
4. Durch die Umgehung der Pointer-Authentifizierung können Angreifer gültige Code-Zeiger fälschen.
5. Der Angreifer leitet die Codeausführung auf eine bösartige Payload um.
6. Das Gerät wird kompromittiert und die Überwachung beginnt.

Was bedeutet das?

- **Es handelt sich um einen gezielten Zero-Click-Angriff:** Der Benutzer muss auf nichts klicken und trotzdem wird sein Gerät kompromittiert. Bei den Betroffenen handelt es sich wahrscheinlich um hochrangige Personen wie Journalisten, Politiker oder Führungskräfte.
- **Und Schwachstellen summieren sich:** Die Angreifer suchen genau nach diesen Schwachstellen, und sie sind wirklich gut darin, sie zu finden.
- **Patches sind wichtig:** Diese Schwachstellen wurden in iOS 18.4.1 behoben. Wenn Ihre Geräte nicht auf dem neuesten Stand sind, sind Ihre Daten nicht geschützt.

Dies zeigt, wie wichtig es ist, Geräte kontinuierlich zu aktualisieren. Das heißt aber nicht, dass dies einfach zu implementieren ist. Es gibt eine Reihe von Gründen, warum ein Benutzer sein Gerät nicht aktualisieren möchte:

- Neue Funktionen/Schnittstelle, die sie nicht nutzen wollen
- Inkompatibilität von Apps mit der neuen OS-Version
- Störung des Arbeitsablaufs/kein Zugriff auf Ressourcen

Wie wir gezeigt haben, ist veraltete Software weit verbreitet, und immer auf dem neuesten Stand zu sein, bleibt eine fortlaufende Herausforderung. Die Implementierung von Aktualisierungsfristen und Mindestversionen des Betriebssystems schützt Ihre Geräteflotte vor schwerwiegenden Schwachstellen, wie die, die 2025 von Jamf Threat Labs analysiert wurden.

Angreifer nutzen die Schwachstellen aus, um Zero-Click-Vektoren wie das Parsen von Bild- und Audiodateien sowie One-Click-Browser-Angriffe zu implementieren. Selbst mit Sicherheitspatches und den Bemühungen der Hersteller sind Angreifer immer noch in der Lage, neue Schwachstellen zu finden und auszunutzen, um offensive Lösungen zu entwickeln. Daher sind regelmäßige Aktualisierungen von mobilen Geräten entscheidend für den Schutz vor Schwachstellen.
Im Folgenden finden Sie einen Überblick über die wichtigsten Schwachstellen aus 2025.

Signifikante iOS-Schwachstellen 2025

CVE-2025-24201 | Schweregrad: 10,0 (kritisch)	CVE-2025-43300 | Schweregrad: 10,0 (kritisch)	CVE-2025-31201 | Schweregrad: 9,8 (kritisch)
BESCHREIBUNG:		
In böser Absicht erstellte Webinhalte können möglicherweise aus der Sandbox für Webinhalte ausbrechen.	Die Verarbeitung einer bösartigen Bilddatei kann zu einer Beschädigung des Speichers führen.	Ein Angreifer mit beliebigen Lese- und Schreibfähigkeiten könnte in der Lage sein, die Pointer-Authentifizierung zu umgehen.
AUSWIRKUNGEN:		
Diese Schwachstelle ermöglicht das Schreiben von Daten außerhalb der Grenzen, also hinter das Ende oder vor den Anfang des vorgesehenen Puffers. Dies kann zu einer Beschädigung des Speichers führen oder es einem Angreifer ermöglichen, Daten zu manipulieren, um beliebigen Code auszuführen.	Diese Schwachstelle ermöglicht das Schreiben von Daten außerhalb der Grenzen, also hinter das Ende oder vor den Anfang des vorgesehenen Puffers.	Diese Schwachstelle beinhaltet fehlerhafte Zugriffsbeschränkungen, wodurch nicht autorisierte Akteure Zugriff auf sensible Systemkomponenten erhalten können. Infolgedessen können Angreifer den Speicher modifizieren und lesen und nicht autorisierten Code ausführen.
GEPATCHTES OS:		
iOS 18.3.2 und iPadOS 18.3.2	iOS 18.6.2 und iPadOS 18.6.2	iOS 18.4.1 und iPadOS 18.4.1

Weitere Schwachstellen, die nach unserer Bestätigung im Jahr 2025 ausgenutzt wurden, sind in der folgenden Tabelle aufgeführt.

iOS

GEPATCHTE IOS-VERSION	DATUM	EINSTUFUNG DER SCHWACHSTELLEN	KOMPONENTE
18.3.1	Februar 2025	CVE-2025-24200 CVSS-Score: 6,1 | Schweregrad: mittel	Zugänglichkeit
18.3.1	Februar 2025	CVE-2025-43200 CVSS-Score: 4,2 | Schweregrad: mittel	Nachrichten
18.4.1	April 2025	CVE-2025-31200 CVSS-Score: 9,8 | Schweregrad: kritisch	CoreAudio
26.2	Dezember 2025	CVE-2025-43529 CVSS-Score: 8,8 | Schweregrad: hoch	WebKit
26.2	Dezember 2025	CVE-2025-14174 CVSS-Score: 8,8 | Schweregrad: hoch	WebKit

Signifikante Android-Schwachstellen 2025

CVE-2025-10585 | Schweregrad: 9,8 (kritisch)	CVE-2025-48543 | Schweregrad: 8.,8 (hoch)	CVE-2024-53104 | Schweregrad: 7,8 (hoch)
BESCHREIBUNG:		
Eine Typverwechslung in V8 in Google Chrome ermöglichte es einem Angreifer, über eine manipulierte HTML-Seite potenziell eine Heap-Beschädigung auszunutzen.	An mehreren Stellen besteht aufgrund eines „Use-after-free"-Fehlers die Möglichkeit, die Chrome-Sandbox zu umgehen und den Android-Systemserver anzugreifen. Dies könnte zu einer lokalen Eskalation der Privilegien führen, ohne dass zusätzliche Ausführungsrechte erforderlich sind. Eine Interaktion des Benutzers ist für die Ausnutzung nicht erforderlich.	media: uvcvideo: Überspringe die Analyse von Frames des Typs UVC_VS_UNDEFINED in uvc_parse_format. Dies kann zu Schreibvorgängen außerhalb des zulässigen Bereichs führen, da Frames dieses Typs bei der Berechnung der Größe des Frame-Puffers in `uvc_parse_streaming` nicht berücksichtigt wurden.
AUSWIRKUNGEN:		
Ein Pointer oder eine andere Ressource wird als ein bestimmter Typ deklariert, greift aber später auf eine Ressource von inkompatiblem Typ zu. Dies kann zu Speicherumschreibungen, Abstürzen und möglicherweise zur Ausführung von Code führen.	Die Verwendung von zuvor freigegebenem Speicher kann gültige Daten beschädigen. Wenn Angreifer bösartige Daten einbringen, bevor der Speicher konsolidiert ist, können sie möglicherweise beliebigen Code ausführen.	Das Schreiben von Daten außerhalb der Grenzen eines Puffers – sei es nach dessen Ende oder vor dessen Beginn – kann zu Speicherkorruption führen oder es einem Angreifer ermöglichen, Daten zu manipulieren, um unerwarteten Code auszuführen.
GEPATCHTES OS:		
Chrome 140.0.7339.155	Android 13, 14, 15, 16	Upstream-Linux-Kernel, Februar 2025

Android

GEPATCHTE ANDROID-VERSION	DATUM	EINSTUFUNG DER SCHWACHSTELLEN	KOMPONENTE
12, 12L, 13, 14, 15	März 2025	CVE-2024-43093 CVSS-Score: 7,3 | Schweregrad: hoch	Framework
Sicherheitshinweis*	März 2025	CVE-2024-50302 CVSS-Score: 5,5 | Schweregrad: mittel	Kernel
Sicherheitshinweis	September 2025	CVE-2025-38352 CVSS-Score: 7,4 | Schweregrad: hoch	Kernel

*Android veröffentlicht keine Betriebssystemversionen für Kernel-Updates. In dem entsprechenden Android-Sicherheitshinweis finden Sie weitere Informationen.

Chrome

GEPATCHTE CHROME-VERSION	DATUM	EINSTUFUNG DER SCHWACHSTELLEN
136.0.7103.125	Mai 2025	CVE-2025-4664 CVSS-Score: 4,3 | Schweregrad: mittel
137.0.7151.72	Juni 2025	CVE-2025-5419 CVSS-Score: 8,8 | Schweregrad: hoch
138.0.7204.63	Juni 2025	CVE-2025-6554 CVSS-Score: 8,1 | Schweregrad: hoch
138.0.7204.157	Juli 2025	CVE-2025-6558 CVSS-Score: 8,8 | Schweregrad: hoch
142.0.7444.175*	Dezember 2025	CVE-2025-13223 CVSS-Score: 8,8 | Schweregrad: hoch
143.0.7499.109	Dezember 2025	CVE-2025-14174 CVSS-Score: 8,8 | Schweregrad: hoch

*Die genannte Version ist für Chrome für Desktop bestimmt.

Die Art und Weise, wie Sie Ihre Geräte konfigurieren, ist entscheidend.

Die modernen Betriebssysteme für Mobilgeräte bieten eine Vielzahl leistungsstarker Funktionen, von denen wir vor fünf Jahren nur träumen konnten. Je mehr Kontrolle man über eine „mobile Flotte“ hat, desto verantwortungsvoller muss man mit Patches und Konfigurationen umgehen.

Sie registrieren Ihre Geräte (hoffentlich) im Mobile Device Management (MDM), um sicherzustellen, dass sie ordnungsgemäß konfiguriert sind. Geräte müssen die Balance zwischen Benutzerfreundlichkeit/Produktivität, Sicherheit und Datenschutz wahren – die richtige Konfiguration ist also nicht immer offensichtlich.

Obwohl dies je nach Risikoprofil und Branche Ihres Unternehmens unterschiedlich sein kann, gibt es einige Standardfunktionen und -konfigurationen, die ein hohes Risiko darstellen und daher blockiert werden sollten:

- Jailbroken-Geräte umgehen die Sicherheitsbeschränkungen von Apple und erlauben dem Benutzer, sein Gerät auf unsichere oder instabile Weise zu verändern. Jedes jailbroken Gerät bietet eine potenzielle Hintertür für Angreifer, um in Ihr System einzudringen.
- Alternative App Marketplaces ermöglichen Benutzern die Installation von Apps außerhalb des App Store oder von Google Play. Alternative App Marketplaces unterliegen nicht den gleichen Sicherheits- und Datenschutzanforderungen, was das Risiko einer bösartigen oder problematischen App erhöht.

TROTZ DIESER RISIKEN ENTDECKTE JAMF THREAT LABS, DASS:

1 von 850
beruflich genutzten Geräten
jailbroken war

2 %
der Unternehmen Geräte mit
alternativen App Marketplaces verwendeten.

Stellungnahme von unserem CISO

Der nachfolgende ganzheitliche Ansatz entschärft die häufigsten Bedrohungen für mobile Geräte: Spyware, kompromittierte oder bösartige Anwendungen und ungepatchte Apps, die ohne das Wissen des Benutzers sensible Unternehmensdaten preisgeben können.

- **Stellen Sie sicher, dass alle mobilen Geräte im MDM registriert sind**, genehmigte Betriebssystemversionen und Updates verwenden und die Sicherheitsgrundlagen erfüllen. Jedes Gerät, das gegen die Konformität verstößt, sollte automatisch von den Unternehmensressourcen isoliert werden, bis das Problem behoben ist. Ein robustes Framework zur Verwaltung von Geräten und Benutzern auf diesen Geräten ist von entscheidender Bedeutung, um potenzielle Malware-Ausbrüche zu stoppen, bevor sie entstehen.
- **Wenn Sie eine agentenbasierte Sicherheit implementieren**, können Sie Ihre Infrastruktur auf Jailbreaks, bösartiges Verhalten und Bedrohungen auf Betriebssystemebene überwachen. Stellen Sie sicher, dass die Telemetriedaten in Ihr SIEM fließen, damit Ihr SOC eine ganzheitliche Sicht auf mobile Bedrohungen sowie den Rest Ihrer Umgebung hat.
- **Aktivieren Sie die DNS-Filterung und den Phishing-Schutz**, um alle Apps auf allen Geräten abzudecken, nicht nur die E-Mails. Dies sollte die Erkennung von „Rogue Wi-Fi“ und Attacker-in-the-Middle-Angriffen einschließen.

App-Risiken

Mobile Apps spielen eine wichtige Rolle bei der Erledigung der Aufgaben Ihrer Mitarbeiter. Wie viele mobile Apps werden in Ihrem Unternehmen bereitgestellt? Diese Apps, egal ob sie von Drittanbietern stammen oder selbst entwickelt wurden, dienen als Einfallstor für Ihre sensiblen Daten.

<1 %

der Unternehmen sind von mobiler Malware betroffen.

Malware für Mobilgeräte ist (verhältnismäßig) selten. Es gibt sie, aber nicht in dem Ausmaß wie bei Computern. Dies ist vor allem auf die moderne Architektur der wichtigsten mobilen Betriebssysteme zurückzuführen, bei denen Sandboxing und kontrollierte App Stores das Risiko verringern, dass bösartige Inhalte auf das Gerät gelangen.

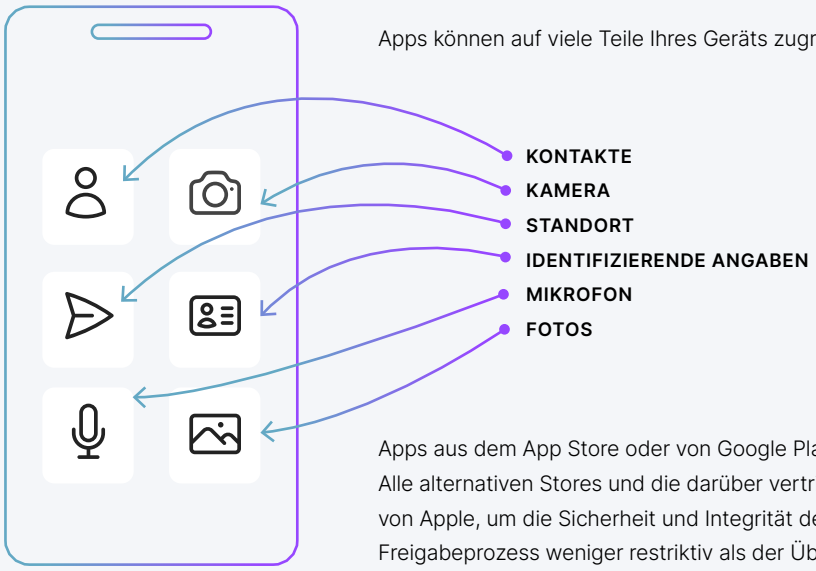
Dennoch vergrößern Apps Ihre Angriffsfläche. Sie sollten Folgendes berücksichtigen:

- **Wie Apps die Speicherung und Übertragung von Daten handhaben**
- **Welche Daten Apps sammeln und wie es um den Datenschutz bestellt ist**
- **Risiken in Bezug auf die Lieferkette, z. B. auf welchen Bibliotheken die App aufbaut**

Böswillige Akteure nutzen Schwachstellen in Apps aus, um fortschrittliche persistente Bedrohungen und Spyware zu implementieren, daher ist ein tiefes Verständnis Ihrer Apps von entscheidender Bedeutung. Außerdem kann die Art und Weise, wie Apps die Datenübertragung über Netzwerke handhaben, ein Risiko darstellen – dazu später mehr.

Die Datenschutzrichtlinien für Apps bestimmen den Umgang mit Daten.

Apps können auf viele Teile Ihres Geräts zugreifen, einige davon sind sensibler als andere:



Apps aus dem App Store oder von Google Play sind verpflichtet, alle gesammelten Daten offenzulegen. Alle alternativen Stores und die darüber vertriebenen Apps unterliegen dem Beglaubigungsprozess von Apple, um die Sicherheit und Integrität der Plattform zu gewährleisten; allerdings ist dieser Freigabeprozess weniger restriktiv als der Überprüfungsprozess im offiziellen App Store.

Sicherheit und Datenschutz sind schwer miteinander zu vereinbaren.

Unabhängig davon, ob Sie Ihren Mitarbeitern mobile Geräte zur Verfügung stellen oder ihnen erlauben, ihr eigenes Gerät mitzubringen, müssen Sie bei der Gewährung des Zugriffs auf die Ressourcen und Daten Ihres Unternehmens der Sicherheit und dem Datenschutz Vorrang einräumen. Sicherheit, denn Sie müssen Ihre Daten schützen. Und Datenschutz, denn Sie müssen den Benutzer schützen.

Dieses Gleichgewicht zu finden, ist nicht immer leicht. Zum Beispiel:

- Ihre **Maßnahmen zur Verhinderung von Datenverlusten** können zu Praktiken führen, die gegen den Datenschutz verstoßen
  .
- **Ein Gerät** aus Sicherheitsgründen zu sperren, kann die Produktivität beeinträchtigen.
- **Unangemessene Richtlinien** können zu einer Schatten-IT führen, bei der Benutzer für bestimmte Aufgaben nicht zugelassene Apps herunterladen.

Um diese Probleme zu bekämpfen, kann Ihre Organisation folgende Regeln einführen:

- Für den Zugriff auf Unternehmensressourcen muss man sich beim **MDM** registrieren
- Persönliche und Unternehmensdaten müssen mithilfe von gehärteten Containern oder Partitionen auf BYOD-Geräten getrennt werden, um Richtlinien zur Vermeidung von Datenverlusten durchzusetzen. Dadurch schützen Sie die Privatsphäre der Benutzer, indem Sie den Zugriff auf persönliche Daten unterbinden.
- Der Datenverkehr im Netzwerk des Unternehmens muss über verschlüsselte Tunnel laufen, um Vertraulichkeit und Datenintegrität zu gewährleisten.
- Benutzer müssen sich über bewährte Sicherheitsverfahren und -richtlinien schulen lassen

Nachtrag: Analyse der App-Sicherheit

Jamf hat sich mit NowSecure zusammengetan, um eine umfassende Analyse des Risikos mobiler Apps durchzuführen, insbesondere in Bezug auf Apps, die bei der Bereitstellung in Unternehmen beliebt sind. Wir haben 135 der beliebtesten und am weitesten verbreiteten Apps für den geschäftlichen und persönlichen Gebrauch auf Mobilgeräten analysiert und dabei den OWASP-Standard als Grundlage für die Risikobewertung von mobilen Apps verwendet.

Alle analysierten Apps waren zum 31. Dezember 2025 auf dem neuesten Stand und spiegeln die reale Situation in Unternehmen mit aktuellen App-Builds wider.

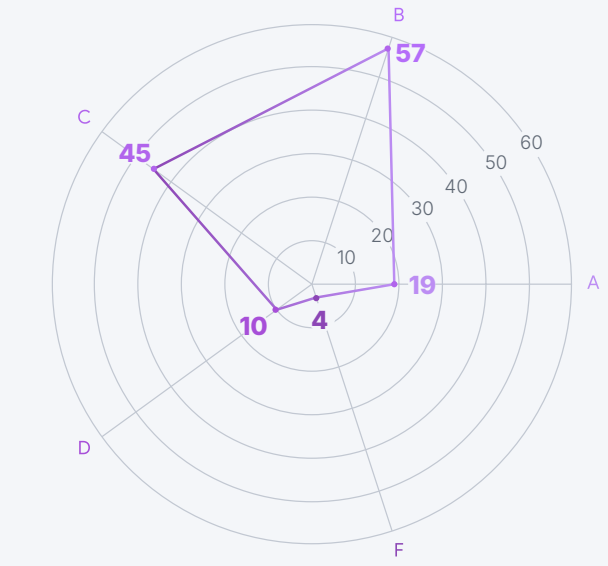
NowSecure unterstützt Unternehmen dabei, zu verhindern, dass Schwachstellen in mobilen Apps und Datenlecks zu Sicherheits-, Datenschutz- oder Konformitätsvorfällen werden. Durch die kontinuierliche Analyse mobiler Apps von Erst- und Drittanbietern und die Einbindung der Ergebnisse in Sicherheits-, IT- und Risiko-Workflows bietet NowSecure den Teams die Transparenz, die Beweise und die Governance, die sie für die Verwaltung mobiler Risiken in großem Umfang benötigen.

Erfahren Sie mehr über NowSecure.

App-Sicherheitsbewertung

NowSecure bietet eine Sicherheitsbewertung für mobile Apps von null bis 100 (je höher, desto besser) und eine Risikobewertung von **A** bis **F** (**A**=minimales Risiko, **F**=erhebliches Risiko). Diese Bewertungen basieren auf automatisierten Tests, bei denen Schwachstellen, Datenlecks, unsichere Kodierungspraktiken, Schwachstellen in der Kryptografie und Netzwerkmängel bewertet werden.

SICHERHEITSSCORES BELIEBTER APPS



A — F
Geringes Risiko — Erhebliches Risiko

Etwa **86 %** der 135 analysierten Apps weisen bekannte Sicherheitslücken auf, wobei nur **14 %** als minimal risikobehaftet eingestuft werden. Dies bedeutet, dass selbst die beliebtesten geschäftlich und privat genutzten Apps in den neuesten Versionen mit Risiken behaftet sind.

VERBREITUNG VON SCHWACHSTELLEN

26 %	73 %	1 %
Niedrig	Mittel	Hoch

Von allen Schwachstellen, die in der Analyse gefunden wurden, fielen die meisten in eine mittlere Schwerekategorie. Wie wir später feststellen werden, übersteigt die Anzahl der Schwachstellen die Anzahl der analysierten Apps. Das bedeutet, dass mehrere Apps mit mehr als einer Schwachstelle behaftet waren.

Bewertung der Schwachstellen einer App

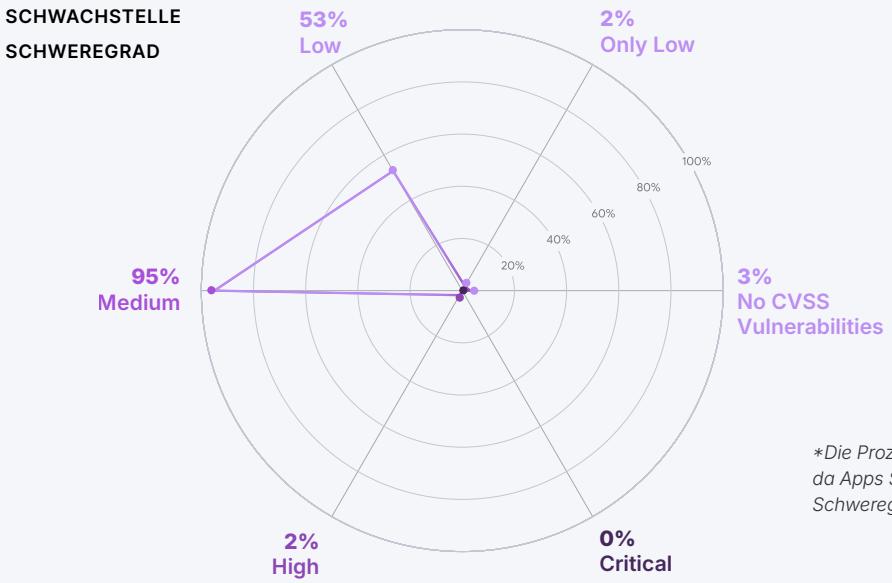
Es ist wichtig, die Risikoauswirkungen zu bewerten, die sich aus der Kombination mehrerer Schwachstellen innerhalb einer einzelnen App ergeben. Zum Zeitpunkt der Bewertung wiesen **95 %** der Apps mindestens eine Schwachstelle mit mittlerem Schweregrad auf, und **2 %** der 135 Apps wiesen Schwachstellen mit hohem Schweregrad auf - und waren damit anfällig für Angriffe.

Während die Softwarehersteller die Schwachstellen in ihren Anwendungen beheben müssen, sind die Unternehmen dafür verantwortlich, ihr Risiko zu verstehen und für rechtzeitige Updates zu sorgen. Es gibt unterschiedliche Empfehlungen für die Patch-Kadenz (z. B. empfiehlt die CISA die Behebung von Schwachstellen mit kritischem Schweregrad innerhalb von 15 Kalendertagen nach der ersten Entdeckung und von Schwachstellen mit hohem Schweregrad innerhalb von 30 Kalendertagen nach der ersten Entdeckung). Diese Daten zeigen, dass alle Unternehmen über Programme verfügen sollten, um Apps auf dem neuesten Stand zu halten.

Wie bereits erwähnt, bewertete NowSecure die Apps anhand ihrer aktuellen Versionen. Die meisten wiesen jedoch mehrere Schwachstellen auf. Das Management von App-Risiken ist eine kontinuierliche, sich ständig weiterentwickelnde Aufgabe, die eine ständige Überwachung und Durchsetzung erfordert.

Aber es ist machbar, wenn Sie diese Aspekte implementieren:

1. Kontinuierliche Ermittlung von Schwachstellen und Fragen zum Datenschutz
2. Priorisierung der Problembehebung auf der Grundlage der geschäftlichen Auswirkungen
3. Durchsetzung von Richtlinien durch Kontrollmechanismen im Mobile Device Management
4. Überwachung des Verhaltens von Drittanbieter-Apps

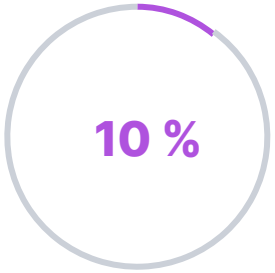


**Die Prozentsätze können 100 % übersteigen, da Apps Schwachstellen in mehreren Schweregraden enthalten können.*

Lieferkette

Mobile Apps stützen sich häufig auf SDKs und Bibliotheken von Drittanbietern, die versteckte Risiken bergen.

Ihre App könnte akzeptable Richtlinien zur Datenerfassung und zum Datenschutz haben, aber Software Development Kits (SDK) oder Bibliotheken von Drittanbietern verwenden, die kritische Mängel aufweisen. Da Unternehmen für die Offenlegung von Daten und die Nichteinhaltung von Vorschriften verantwortlich sind, müssen sie sich einen Überblick über die Risiken in der Software-Lieferkette verschaffen.



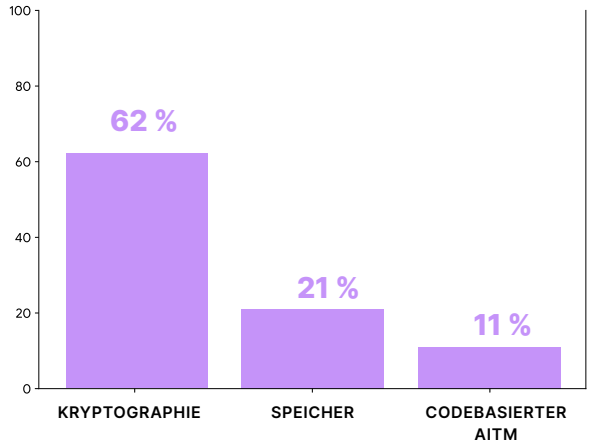
der **Apps**, die **anfällige Bibliotheken** verwenden

Sicherheit der Daten

Daten können auf verschiedene Weise aus Apps abfließen.

- **Probleme mit der Kryptographie:** Für App-Entwickler ist es schwierig, Daten zu sichern, die Kommunikation zu schützen und die Identität der Benutzer zu überprüfen. Viele verlassen sich auf Bibliotheken von Drittanbietern. Bei allen analysierten Apps stellte NowSecure die Verwendung von zwei bekannten unsicheren Bibliotheken fest: OpenSSL und libpng.
- **Unsichere Speicherung:** Die Art und Weise, wie Daten im Speicher verwaltet werden, kann über die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten entscheiden. Unzureichende Schutzmaßnahmen bei der Speicherung erhöhen das Risiko der Exfiltration von Daten.
- **AitM-Risiken:** Auch die Art und Weise, wie Apps mit Daten während der Übertragung umgehen, ist wichtig. Wenn die Kommunikation nicht ordnungsgemäß verschlüsselt ist, kann ein Angreifer beispielsweise sensible Daten während der Übertragung abfangen oder manipulieren.
- **Zugriff auf Daten:** Mobile Apps haben Zugriff auf Cloud- und Unternehmensdaten, die sehr lukrativ für Angreifer sind. Datenverlust ist Datenverlust, unabhängig davon, wie auf die Daten zugegriffen wurde.

ARTEN VON SCHWACHSTELLEN



KI-Nutzung

KI, insbesondere generative KI, ist derzeit ein heißes Thema. In einem Bericht vom Januar 2026 stellt Deloitte fest, dass der Zugang von Arbeitnehmern zu sanktionierter KI innerhalb eines Jahres um 50 % gestiegen ist, wobei 60 % der Mitarbeiter KI-Tools bei der Arbeit nutzen.

Das macht Sinn, denn sowohl die KI auf dem Gerät als auch die Cloud-basierte KI bieten eine Vielzahl von praktischen Funktionen. Mobile Apps zum Beispiel enthalten zunehmend beides:

- **KI auf dem Gerät:** Mit großen Sprachmodellen können Anwendungen natürliche Sprache verarbeiten, wie z. B. Texterstellung und prädiktive Eingabe, während Machine Learning-Modelle für Funktionen wie Bilderkennung, Objekterkennung in Echtzeit, Barcode-Scanner und Augmented Reality verwendet werden.
- **Cloud-basierte KI:** Ausführung komplexer Aufgabenstellungen, die auf eine externe Infrastruktur für die Verarbeitung und Berechnung angewiesen sind.

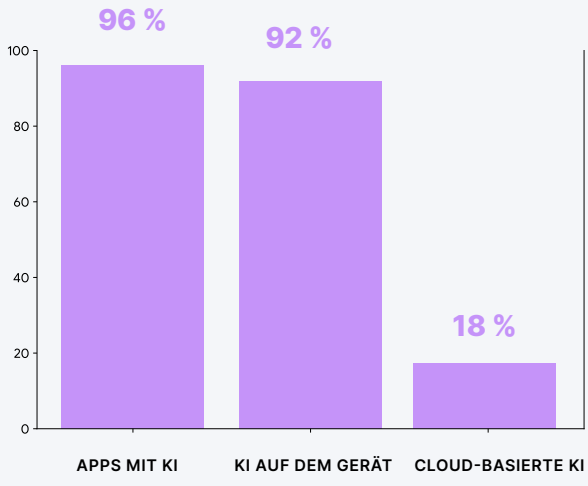
Benutzer und Unternehmen nehmen generative KI schnell an, aber so schnell wie sich die Technologie weiterentwickelt, so schnell steigen auch die Risiken.

Bedenken Sie die Risiken:

- Benutzer können Schatten-KI verwenden, d. h. einen nicht genehmigten und unkontrollierten KI-Zugriff, der **sensible Unternehmensdaten** enthalten und gegen Richtlinien verstoßen kann. Die Abhängigkeit der Cloud-basierter KI von einer externen Infrastruktur bedeutet, dass Ihr Unternehmen möglicherweise keine Transparenz über die **potenziellen Risiken** hat, einschließlich der **Offenlegung von Daten**.
- Benutzer können KI-Agenten einsetzen, um **autonome Aktionen durchzuführen**, die über die vorgesehenen Kontrollen hinausgehen.

Es stellt sich heraus, dass viele gängige Apps KI verwenden, oft ohne klare Transparenz für das Unternehmen.

PRÄSENZ VON KI-FUNKTIONEN IN APPS



Datenschutz

Wir nehmen unsere mobilen Geräte überallhin mit. Sie enthalten eine Vielzahl von Informationen über unser Privat- und Arbeitsleben: Fotos, Kontakte, sensible Daten, Finanzdokumente, geschützte Informationen usw.

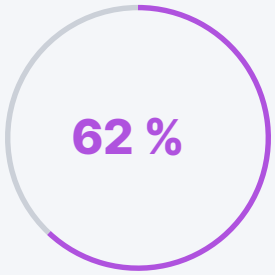
Aus diesem Grund legen Benutzer und Arbeitgeber großen Wert auf den Datenschutz. Außerdem unterliegen Sie möglicherweise den Datenschutzgesetzen.

Dies spiegelt sich jedoch nicht immer in unseren Apps wider, sei es durch die Absicht des Entwicklers oder durch Nachlässigkeit. Apps können gefährliche Berechtigungen anfordern, die sensible Daten sammeln, wie z. B. den Zugriff auf:

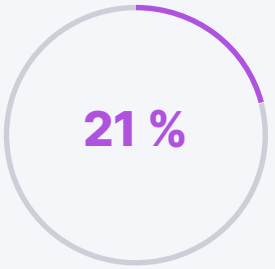
- Standort des Geräts
- Mikrofon
- Kamera
- Kontakte

Wie gehen Apps über das Anfordern von Informationen hinaus mit ihnen um? Einige Daten werden erfasst, weil die App sie zum Funktionieren benötigt. Andere Daten nicht so sehr. Bestimmte App-Funktionen untergraben den Datenschutz, z. B:

- Tracking und Erstellung von Profilen
- Datenfreigabe mit Dritten
- Erfassung von Kontaktdaten/gezielte Werbung



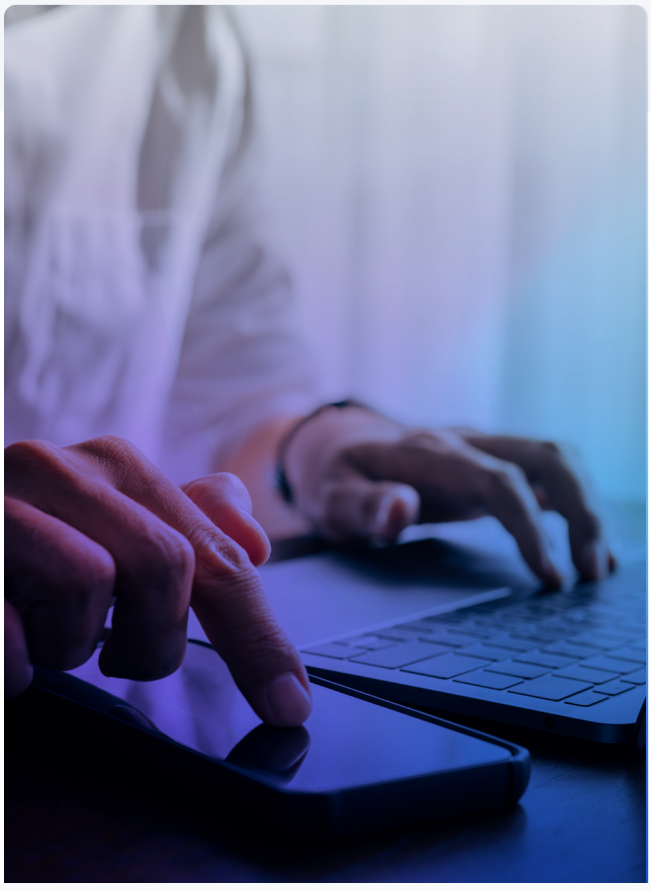
der **Apps**, die gefährliche Berechtigungen anfordern



der **Apps** enthielten datenschutzrelevante Verhaltensweisen

Stellungnahme von unserem CISO

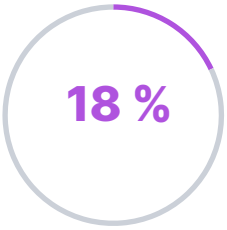
Mobile Apps sind das Eingangstor zu sensiblen Unternehmensdaten. Um dieses Risiko in den Griff zu bekommen, müssen Unternehmen kontrollieren, welche Apps auf den Geräten zugelassen sind, Daten bei der Übertragung über Netzwerke schützen und die Schwachstellen der Apps in der gesamten Geräteflotte im Blick behalten. Bei BYOD ist das Ziel die Trennung. Es geht um Containerisierung und Schutz von Unternehmensdaten, ohne den persönlichen Datenschutz zu verletzen. Das Ergebnis ist ein ausgewogener Ansatz, bei dem die Sicherheitsteams über die erforderlichen Kontrollen verfügen und die Mitarbeiter darauf vertrauen können, dass ihre persönlichen Daten vertraulich bleiben.



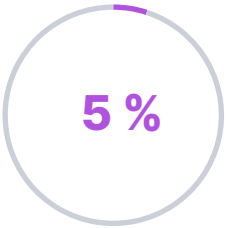
Netzwerk- und Web-Risiken

Eins ist klar: Angreifer werden sich auch weiterhin auf die schwächste Stelle in unserer Sicherheit konzentrieren: den Faktor Mensch. Und sie werden immer besser und nutzen generative KI, um immer überzeugendere Angriffe zu entwickeln. Benutzer klicken auf Phishing-Links, verbinden sich mit riskanten WLAN-Netzwerken und Hotspots und vernachlässigen ihre Cyber-Hygiene.

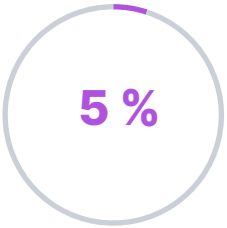
Nicht alle Schwachstellen befinden sich auf dem Gerät; selbst perfekt gesicherte Geräte mit idealen Konfigurationen bleiben anfällig für Bedrohungen, die Daten bei der Übertragung abfangen. Deswegen sind Netzwerke sind ein beliebtes Ziel. Dies kann sich auf verschiedene Weise zeigen:



der **Unternehmen** haben Benutzer, die sich mit riskanten Hotspots verbinden



der **Unternehmen** haben Benutzer, die Opfer von infrastrukturbasierten AitM-Angriffen geworden sind



der **Unternehmen** haben Geräte, die von Cryptojacking betroffen ist

Netzwerkinfrastruktur

Sie können die Konfigurationen Ihres eigenen Netzwerks kontrollieren, aber nicht alle Netzwerke von Drittanbietern – einschließlich mobiler Netzwerke –, mit denen sich Ihre Benutzer außerhalb Ihres Verantwortungsbereichs verbinden. Hoffentlich erzwingen Sie bedingten Zugriff, segmentieren Ihr Netzwerk und setzen Richtlinien für den Zero-Trust-Netzwerkzugriff durch.

Andernfalls sind Ihre Daten in Gefahr. Wenn ein Benutzer eine Verbindung zu einem ungesicherten öffentlichen WLAN-Netzwerk herstellt, das möglicherweise eine schwache Verschlüsselung oder keine Authentifizierung aufweist, können Angreifer dies ausnutzen, um Session-Cookies zu stehlen, die Zertifikatsvalidierung zu umgehen oder andere Techniken anzuwenden.

Webprotokolle regeln, wie Geräte, Browser und Server Informationen austauschen. Sie sind ein wichtiger Bestandteil der Datensicherheit. Angreifer können diese Protokolle zu älteren, weniger sicheren Versionen herabstufen und so die Entschlüsselung und den Diebstahl von Daten während der Übertragung erleichtern. Dies macht Ihr Unternehmen anfällig für „Adversary-in-the-Middle“-Angriffe.

Diese AitM-Angriffe nutzen Schwachstellen in der Netzwerkinfrastruktur aus, im Gegensatz zu codebasierten Schwachstellen in einem Betriebssystem oder einer App.

Web-Risiken

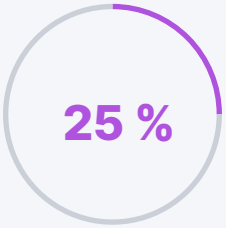
Selbst bei einer sicheren Verbindung ist das Surfen im Internet nicht immer sicher. Ein Gerät muss nicht unbedingt gefährdet sein, um zum Sicherheitsproblem zu werden. Das Anklicken bösartiger Links/Werbung oder das Aufrufen problematischer Websites kann zu Cryptojacking und dem Abfangen von Anmeldedaten über Phishing führen. Cryptojacking – bei dem Angreifer die Verarbeitungs- und Speicherressourcen eines Geräts nutzen, um Kryptowährungen zu schürfen – kann ein Gerät bis zur Unbrauchbarkeit verlangsamen.

Ah, Phishing, unser allseits beliebter Feind. Generative KI macht es jetzt noch einfacher, eine überzeugende Phishing-Nachricht zu erstellen. Benutzer können nicht mehr davon ausgehen, dass böswillige Nachrichten mit Tippfehlern und anderen klassischen Erkennungsmerkmalen behaftet sind.

Die 30 häufigsten Marken, die in Phishing-Kampagnen verwendet werden

Bösewichte imitieren gerne bekannte Marken. Benutzer klicken eher auf einen Link von einem Dienst, den sie nutzen und mit dem sie vertraut sind - Angreifer nutzen das Vertrauen der Benutzer in die Institutionen aus, die sie täglich nutzen. Für Angreifer besteht ein besonderer Anreiz, Banken und Finanzdienstleistungen ins Visier zu nehmen, da kompromittierte Accounts wahrscheinlich sowohl Geld als auch sensible Daten enthalten.

Beachten Sie, dass diese Marken nichts Böses getan haben; aber die Angreifer nutzen ihren vertrauenswürdigen Ruf aus, um ahnungslose Benutzer in einen Hinterhalt zu locken.



der **Organisationen** melden einen Benutzer, der auf einen Phishing-Link hereingefallen ist.

Unterhaltung/ Vernetzung	Business	Dienstprogramm	Bankwesen/ Finanzdienstleistungen
Netflix	Microsoft	Optus	Allegro
Facebook	Apple	AT&T	U.S. Internal Revenue Service
Steam	Adobe	Amazon	Rakuten
eBay, Inc.		DHL	Coinbase
WhatsApp		British Telcom	PayPal
		Orange	AEON Card
		Comcast	Sumitomo Mitsui Banking Corporation
		East Japan Railway Company	Navy Federal Credit Union
			Bradesco
			Bank of America Corporation
			HSBC Group
			Raiffeisen Bank
			American Express
			ING Direct

Stellungnahme von unserem CISO

Zusätzlich zu den technischen Kontrollen ist es wichtig, die Mitarbeiter proaktiv darauf zu schulen, Phishing und andere Social-Engineering-Bedrohungen zu erkennen und zu melden. Dazu eignen sich Sensibilisierungsprogramme, Schulungen und Phishing-Tests. Phishing-Tests sollten KI nutzen, um die Simulationen auf die Fähigkeiten der Benutzer zuzuschneiden und sie angesichts neuer und vielfältiger Bedrohungen aktuell zu halten.

Die Ausbreitung von Risiken: fortgeschrittene anhaltende Bedrohungen

Bisher haben wir über die Risiken gesprochen, die damit verbunden sind:

- Betriebssystem und Konfiguration der Geräte
- Mobile Apps
- Networking und Surfen im Internet

Jedes einzelne Risiko, z. B. eine Schwachstelle im Betriebssystem, eine mobile App mit suboptimaler Datenverarbeitung oder ein Benutzer, der sich mit einem öffentlichen WLAN verbindet, kann erhebliche Auswirkungen auf Ihre Datensicherheit haben.
Oder auch nicht, je nach Ihren Konfigurationsrichtlinien und Schulungen für die Benutzer.

Doch wenn sich diese Risiken häufen, werden sie zu einem Problem. Fortgeschrittene Bedrohungsgruppen kombinieren mehrere Schwachstellen, um komplexe Exploits zu entwickeln. Während die für diese fortgeschrittenen Angriffe verantwortlichen Akteure in der Vergangenheit Zurückhaltung zeigten und sich auf hochkarätige Ziele konzentrierten, werden ihre Toolkits nun zunehmend breiter gestreut, was potenziell auch Durchschnittsbürger in Gefahr bringt.

Das Verständnis dieser fortschrittlichen Bedrohungen ist eine wesentliche Voraussetzung für die Abwehr dieser Bedrohungen. Jamf Threat Labs bewertete die verschiedenen Mechanismen zur Ausnutzung von Angriffen (einschließlich Zero-Click- und One-Click-Angriffen) und die Modelle zur Bereitstellung von Daten, die bei gezielten Überwachungsmaßnahmen verwendet werden, um Daten von hochgefährdeten Benutzern wie Journalisten, Führungskräften von Unternehmen, Politikern, Aktivisten und anderen zu erhalten. Die Analyse umfasst Themen wie Schwachstellen in Betriebssystemen und Apps von Drittanbietern sowie die entsprechenden Reaktionen der Anbieter. Das haben sie herausgefunden.

So schützen Sie Ihr Unternehmen
Implementieren Sie Maßnahmen zur Erkennung nach einem Angriff, Verhaltensdaten und anomaliebasierte Überwachung ein, anstatt sich allein auf Kontrollen der Benutzerinteraktion zu verlassen.

Zero-Click-Angriffe bleiben hochrelevant

Zero-Click-Angriffe auf Apple- und Android-Geräte bleiben auch 2025 ein aktiver Bedrohungsvektor, insbesondere für Journalisten und leitende Angestellte. Dies wird durch die Entdeckung eines Angriffs auf WhatsApp-Benutzer untermauert, der eine Schwachstelle bei der Bildverarbeitung (CVE-2025-43300) ausnutzte.

Dieser Fund belegt, dass es Angreifern nach wie vor gelingt, Schadcode ohne Zutun des Anwenders auszuführen, wodurch herkömmliche Abwehrmechanismen wirkungslos werden. Diese Angriffe stehen in der Regel im Zusammenhang mit gezielten Überwachungs- oder Aufklärungsmaßnahmen.

Das kontinuierliche Auftreten von Zero-Click-Schwachstellen in der Praxis bestätigt, dass motivierte Angreifer sowohl die Fähigkeit als auch die Absicht haben, in die kostspielige Entwicklung von Schwachstellen zu investieren.

Es gibt weiterhin Browser-Angriffe, einschließlich der heimlichen Verbreitung über Werbung.

Apple und Google haben im Laufe des Jahres zahlreiche Sicherheitspatches für ihre Browser veröffentlicht. Chrome erhielt 250 Sicherheitspatches, Safari über 75, was darauf hinweist, dass kontinuierlich Sicherheitslücken im Speicherbereich identifiziert werden, die durch manipulierte Webinhalte ausgelöst werden können.

Diese Schwachstellen sind besonders interessant, weil sie über JavaScript auf bösartigen Websites oder in Werbeanzeigen als Waffe eingesetzt werden können, was die Betriebskosten für Angreifer senkt. Berichte über Bedrohungsdaten bestätigen, dass Anbieter kommerzieller Spyware weiterhin auf One-Click-Exploit-Ketten setzen, bei denen sie ausgenutzte Sicherheitslücken mit Sandbox-Escape-Techniken kombinieren, um die vollständige Kontrolle über das Gerät zu erlangen.

Die Entdeckung der Aktivitäten von Intellexa macht deutlich, dass solche Exploits von Geheimdiensten aktiv genutzt werden und auch als Zero-Click-Angriffe über ein Netzwerk von Werbeträgern verbreitet werden können.

WIE SIE IHR UNTERNEHMEN SCHÜTZEN KÖNNEN:
Erweitern Sie Ihre Sicherheitsarchitektur um die Überprüfung des Webdatenverkehrs, die Erkennung von Exploit-Verhalten sowie die forcierte, schnelle Aktualisierung von Betriebssystemen und Browsern in verwalteten Mobilumgebungen.

Die ins Visier genommenen Unternehmen wehren sich aktiv, aber die Abwehrmaßnahmen sind nach wie vor unzureichend.

Im Jahr 2025 verstärkten Plattformanbieter und große Technologieunternehmen nachweislich ihre Bemühungen zur Bekämpfung gezielter Spyware-Operationen, einschließlich rechtlicher, technischer und architektonischer Maßnahmen. Aufsehenerregende Gerichtsverfahren, wie das von Meta gegen die NSO Group, verdeutlichen eine Eskalation, die über rein technische Abwehrmaßnahmen hinausgeht und zu einer nachhaltigen rechtlichen Abschreckung führt.

Gleichzeitig investiert Apple weiterhin in Abhilfemaßnahmen auf Plattformebene, darunter die Memory Tagging Extension (MTE) und die Verbesserung des Blockierungsmodus. Doch trotz dieser Maßnahmen gibt es weiterhin erfolgreiche Ausbeutungsketten.

Fortgeschrittene Angreifer passen ihre Werkzeuge und Techniken immer weiter an, um neue Schutzmechanismen zu unterlaufen. So wurde kürzlich auf einer privaten Konferenz eine mögliche Umgehungslösung vorgestellt.

WIE SIE IHR UNTERNEHMEN SCHÜTZEN KÖNNEN:
Ergänzen Sie herstellerspezifische Schutzmaßnahmen durch unabhängige Erkennungssysteme, forensische Nachvollziehbarkeit sowie Kapazitäten zur Reaktion auf Sicherheitsvorfälle, die speziell auf gezielte Angriffsszenarien zugeschnitten sind.

Spyware, auf die Sie achten sollten

Predator | Entwickler: Intellexa

Predator nutzt in erster Linie webbasierte One-Click-Exploits, die häufig über bösartige Links oder Webinhalte, einschließlich Werbung, verbreitet werden. Dabei werden Schwachstellen in WebKit ausgenutzt, wie die wiederholten Patches von Apple zeigen. Dieses Modell ist besser skalierbar, reagiert aber empfindlicher auf die Patch-Latenz. Predator zeigt, dass One-Click-Angriffe weiterhin möglich sind.

Graphite | Entwickler: Paragon

Graphite ist eine kommerzielle Spyware-Plattform, die mit der fortgeschrittenen Ausnutzung von iOS verbunden ist und sowohl Zero-Click- als auch One-Click-Delivery unterstützt. 2025 demonstrierte ein erfolgreicher Zero-Click-iMessage-Angriff auf vollständig gepatchte iPhones die Fähigkeit von Graphite, Geräte ohne Benutzerinteraktion zu kompromittieren. Mehrere Kompromittierungen wurden derselben Betreiberinfrastruktur zugeschrieben, was bestätigt, dass es sich um eine koordinierte und gezielte Ansteckung und nicht um opportunistische Aktivitäten handelt. Dadurch etabliert sich Graphite als operativer Nachfolger auf dem Spyware-Markt, ungeachtet des gestiegenen regulatorischen und rechtlichen Drucks auf die Anbieter.

Landfall | Entwickler: N/A

Landfall ist eine bisher unbekannte, kommerzielle Android-Spyware-Familie, die in einer gezielten Spionagekampagne gegen Samsung Galaxy-Geräte eingesetzt wird. Die Betreiber nutzten eine kritische Zero-Day-Schwachstelle in der Bildverarbeitungsbibliothek von Samsung aus, um die Spyware über bösartige Bilddateien zu verbreiten, die offenbar über Messaging-Apps wie WhatsApp verbreitet wurden.

Die Kampagne, die mindestens von Mitte 2024 bis zur Behebung der Schwachstelle durch Samsung im April 2025 aktiv war, verschaffte Angreifern umfassende Überwachungsmöglichkeiten – darunter Audioaufnahmen, Standortverfolgung sowie das Abschöpfen von Kontakten, Fotos und Anruflisten. Aus sicherheitstechnischer Sicht zeigt Landfall, dass sich Android-Spyware, die Zero-Day-Schwachstellen ausnutzt, weiterhin außerhalb der öffentlichen Wahrnehmung weiterentwickelt, was die Notwendigkeit eines proaktiven Patch-Managements, der Erkennung von Anomalien und einer langfristigen Gerätetelemetrie auf allen mobilen Plattformen unterstreicht.

Pegasus | Entwickler: NSO Group

Pegasus ist eine High-End-Spyware-Plattform für iOS und Android, die mit Zero-Click- und begrenzten One-Click-Exploit-Ketten verbunden ist und zu eine vollständigen Kompromittierung der Geräte führt. Er zielt auf eine kleine Anzahl hochrangiger Personen ab und ist auf Unauffälligkeit und Langlebigkeit ausgelegt. Im Jahr 2025 wurde die Geschäftstätigkeit von NSO durch Ausfuhrbeschränkungen und rechtliche Verpflichtungen beeinträchtigt. Das Unternehmen wurde inzwischen von einer Investorengruppe übernommen, aber es wird erwartet, dass die Technologie weiterhin von Geheimdiensten genutzt wird, vielleicht unter einem anderen Namen.

Dante | Entwickler: Memento Labs

Memento Labs ist ein italienischer Anbieter von Überwachungstechnologien und Nachfolger des umstrittenen Hacking Teams, das nach seiner Übernahme im Jahr 2019 umbenannt wurde. 2025 wurden Tools, die mit Memento Labs in Verbindung stehen, in einer hochentwickelten Cyberspionage-Kampagne namens Operation ForumTroll verwendet, die eine Zero-Day-Schwachstelle in der Chrome-Sandbox ausnutzte (CVE-2025-2783). Laut ihrem CEO haben sie den Support für Windows-Lösungen eingestellt und ihren Fokus auf mobile Plattformen verlagert; daher ist zu erwarten, dass diese Malware-Familie und die entsprechenden Schwachstellen auf Android-Geräten zu finden sind.

Spyrtacus | Entwickler: SIO

Spyrtacus ist eine kommerzielle Spyware-Familie, die Berichten zufolge im Jahr 2025 aktiv auf Android-Geräte abzielt. Die Spyware wurde über bösartige Links und Social Engineering auf der Anwendungsebene verbreitet. Sobald sie auf einem Gerät installiert ist, verfügt Spyrtacus über typische Spyware-Funktionen wie Datenexfiltration, Standortverfolgung sowie das Abschöpfen von Nachrichten und Kontakten.

Im Gegensatz zu Zero-Click-Spyware wie Pegasus oder Graphite erfordert Spyrtacus in der Regel ein gewisses Maß an Benutzerinteraktion oder Social Engineering, um die Installation einzuleiten. Das Vorhandensein von Spyrtacus in realen Kampagnen unterstreicht, dass nicht jede gezielte mobile Spyware auf Zero-Day-Ausbeutung beruht; stattdessen können Angreifer Social Engineering mit handelsüblichen Spyware-Frameworks kombinieren, um ähnliche Ziele zu erreichen.

Stellungnahme von unserem CISO

Trotz erheblicher Korrekturmaßnahmen auf Plattformebene und Sicherheitshärtung durch die Hersteller entdeckten Angreifer auch 2025 kritische Schwachstellen und nutzten diese aus, insbesondere in wichtigen Komponenten wie Browsern (Chrome, Safari) und Messaging-Apps. Diese Komponenten bleiben aufgrund ihrer Komplexität, ihrer häufigen Exposition gegenüber nicht vertrauenswürdigen Inhalten und ihrer zentralen Rolle in den täglichen Arbeitsabläufen der Benutzer attraktive Angriffsziele.

Die anhaltende Erfolgsserie gezielter Angriffe macht deutlich, dass keine Schutzstrategie das Risiko vollständig beseitigen kann, insbesondere nicht gegenüber Angreifern, die über umfangreiche Ressourcen verfügen. Daher gehören eine rigorose Verwaltung der Geräte und die Durchsetzung von Updates zu den wirksamsten und am besten kontrollierbaren Abwehrmaßnahmen, die Unternehmen zur Verfügung stehen.

Außerdem demonstriert dies, dass das Mobile Device Management keine unterstützende Funktion, sondern eine zentrale Sicherheitsmaßnahme ist. Die Bereitstellung schneller Sicherheitsupdates, die Durchsetzung von Sicherheitsstandards, die Aufrechterhaltung der Geräteübersicht und die Verkürzung von Sicherheitslücken sind entscheidende Faktoren, um die Auswirkungen neu entdeckter Sicherheitslücken zu begrenzen.

Die Risiken sind groß – aber nicht unüberwindbar.

Die Bewältigung dieser Risiken erfordert eine durchdachte Architektur. Die Säulen für sichere Geräte sind:

Geräteverwaltung zur Anwendung von Einschränkungen, Konfigurationen und zur Durchsetzung von Richtlinien

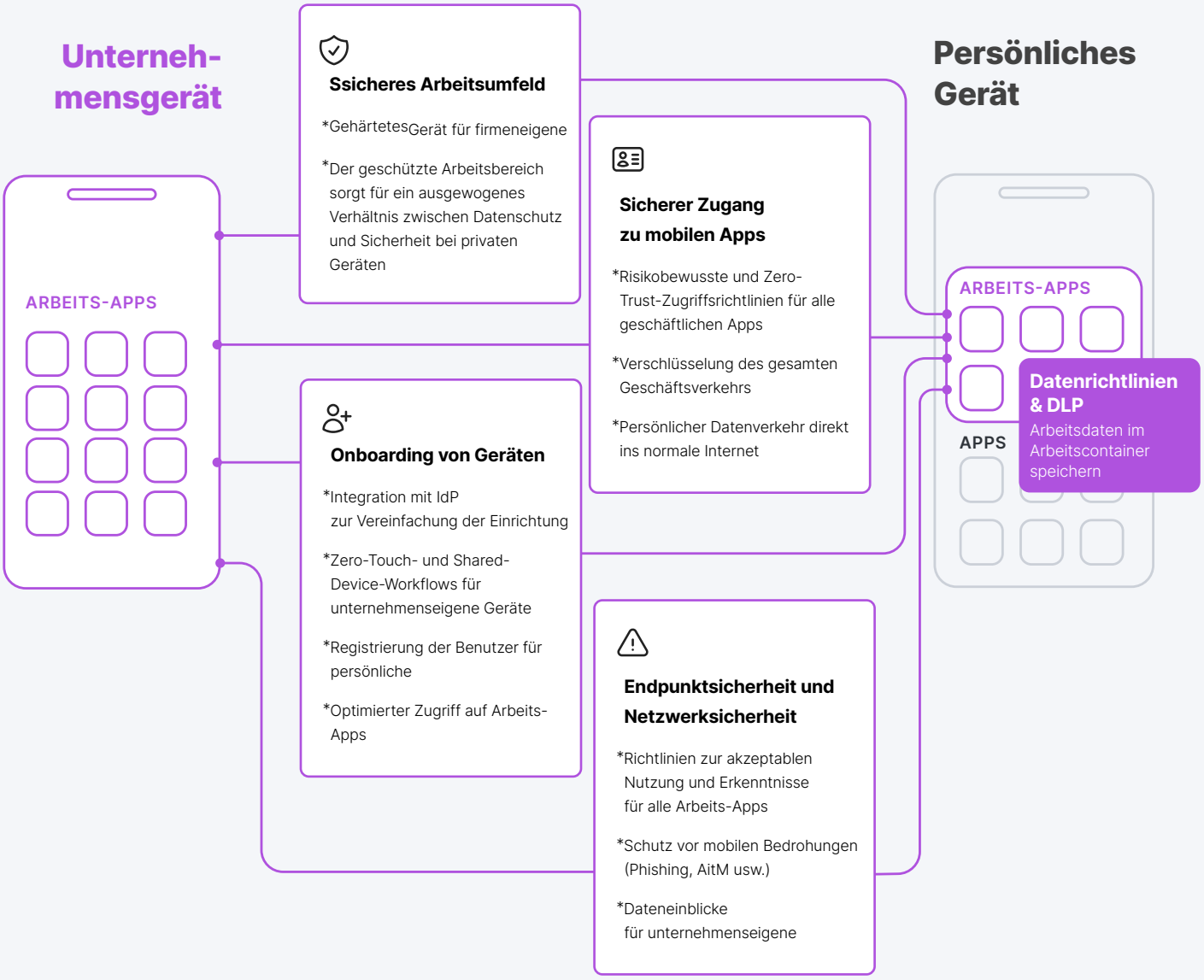
Endpunktsicherheit zur Überwachung des Zustands und Verhaltens des Geräts im Falle einer möglichen Kompromittierung

Sicherer Fernzugriff, um zu steuern, welche Geräte auf Unternehmensressourcen zugreifen können und welche nicht

Diese arbeiten zusammen, um sicherzustellen, dass nur ein konformes Gerät und ein autorisierter Benutzer auf Ihre sensiblen Daten zugreifen kann.

Je nachdem, ob ein **Gerät dem Unternehmen gehört**, kann dies etwas anders aussehen.

Die Konfiguration Ihrer Geräte kann ein Risiko sein - oder ein Gewinn für Ihre Sicherheit. Durch die Automatisierung von Updates, die Überprüfung von Apps und Verhaltensanalysen sowie die Durchsetzung von Zugriffsrichtlinien auf der Grundlage des Konformitätsstatus sind Sie auf dem besten Weg zu einem umfassenden Datenschutz.



Lesen Sie die neuesten Forschungsergebnisse zu Mobilgeräten von Jamf Threat Labs

Wie Predator-Spyware die Aufzeichnungsindikatoren von iOS umgeht

FEBRUAR 2026

Mithilfe einer ausgeklügelten Technik, die sich die „Nil-Messaging"-Funktion von Objective-C zunutze macht, umgeht Predator die Aufzeichnungsindikatoren von iOS. Die Malware klinkt sich in eine einzige SpringBoard-Methode ein, die alle Sensoraktivitätsaktualisierungen verarbeitet, und setzt dann den Selbstzeiger auf NULL, so dass die Indikatoraktualisierungen stillschweigend ignoriert und den Benutzern nicht angezeigt werden. Dieser Ansatz ist subtiler als frühere Techniken, da das Gerät normal funktioniert und keine visuelle Warnung über die Überwachung ausgibt, was einen verdeckten Kamera- und Mikrofonzugriff auf vollständig kompromittierte Geräte ermöglicht.

OpenClaw: die nützliche KI, die heimlich zu Ihrer größten Insider-Bedrohung werden könnte

FEBRUAR 2026

OpenClaw ist ein Open-Source-Framework für die Entwicklung autonomer KI-Agenten, die Shell-Befehle ausführen, auf Dateien zugreifen und mit Apps interagieren können, ohne über integrierte Sicherheitsbarrieren zu verfügen. Dadurch entstehen erhebliche Sicherheitsrisiken für Unternehmen. Das Framework stellt aufgrund des uneingeschränkten Systemzugriffs, dem Potenzial zur Exfiltration von Daten und den Schwachstellen bei indirekten Prompt-Injection-Angriffen, bei denen bösartige Anweisungen in legitime Geschäftsinhalte eingebettet werden, ein Sicherheitsrisiko dar. Jüngste Sicherheitshinweise haben gezeigt, wie Angreifer verschiedene Schwachstellen ausnutzen können, um sich dauerhaften Zugang zu verschaffen. Dadurch stellen OpenClaw-Implementierungen eine hochriskante Insider-Bedrohung dar, deren sichere Verwaltung in Unternehmensumgebungen umfassende Strategien zur Erkennung, Prävention und Governance erfordert.

Der Kill-Switch von Predator: undokumentierte Anti-Analyse-Verfahren in iOS-Spyware

JANUAR 2026

Die Predator-Spyware verfügt über ausgefeilte Funktionen zur Umgehung von Analysen, die weit über bisher dokumentierte Erkenntnisse hinausgehen, darunter ein Fehlercodesystem, das den Betreibern genaue Diagnoseinformationen darüber liefert, warum die Bereitstellung fehlschlägt. Die Malware erkennt den Entwicklermodus, Jailbreak-Tools, Sicherheitsanwendungen und geografische Beschränkungen und nutzt fortschrittliche Anti-Forensik-Maßnahmen, um Aufzeichnungshinweise vor den Opfern zu verbergen.

Diese Mechanismen zeigen, dass die Betreiber detailliertes Feedback erhalten, wenn die Zielerfassung fehlschlägt, was ihnen ermöglicht, Fehler zu beheben und ihre Vorgehensweise anzupassen. Dies belegt, dass kommerzielle Spyware-Anbieter erhebliche Anstrengungen darauf verwenden, Forscher aufzuspüren, und nicht nur darauf, Sicherheitsprodukten zu entgehen.

Jamf Threat Labs hat herausgefunden, dass ein Handyspiel Anmeldedaten von Spielern preisgibt

NOVEMBER 2025

Bei „World of Warships Blitz", einem beliebten Handyspiel mit über 10 Millionen Downloads, wurde festgestellt, dass bei der Anmeldung und Registrierung Anmeldedaten und Sitzungstoken über unverschlüsselte HTTP-Verbindungen offengelegt wurden. Obwohl die Anmeldedaten verschleiert waren, ermöglichte die Datenpanne Replay-Angriffe, bei denen Angreifer Authentifizierungsanfragen abfangen und erneut senden konnten, um Konten zu kapern. Nach einer verantwortungsvollen Offenlegung hat der Entwickler das Problem in Version 8.4.0 behoben.

Diese Untersuchung unterstreicht, dass selbst beliebte Apps kritische Schwachstellen enthalten können und dass mehrschichtige Sicherheitsmaßnahmen und die Aufklärung der Benutzer über Passworthygiene von größter Bedeutung sind.

Jamf Threat Labs hat entdeckt, dass Apps die Anmeldedaten preisgeben

SEPTEMBER 2025

Es wurde festgestellt, dass zwei mobile Apps Benutzerdaten und personenbezogene Daten über unverschlüsselte HTTP-Verbindungen weitergaben – eine malaysische App für das Gesundheitsmanagement mit 15 Millionen Benutzern und die „Spar“-App eines indischen Schmuckunternehmens. Beide Apps übertragen sensible Daten im Klartext, wodurch Benutzer dem Risiko von Datendiebstahl, Identitätsbetrug und unbefugtem Kontozugriff ausgesetzt sind, insbesondere in öffentlichen Netzwerken.

Diese Entdeckung macht deutlich, wie wichtig es für Unternehmen ist, eine sichere Datenübertragung zu implementieren, und für Benutzer, mobile Lösungen zur Abwehr von Bedrohungen, ZTNA und Inhaltsfilterung zu nutzen, um riskante Apps zu blockieren.

Flekst0re: Bewertung der Sicherheit von alternativen App Stores

AUGUST 2025

Drittanbieter-App-Stores für iOS wie Flekst0re bergen erhebliche Sicherheitsrisiken, wie ein manipuliertes WhatsApp-Proof-of-Concept gezeigt hat, das Gespräche heimlich aufzeichnete und an einen Remote-Server übertrug, während es gleichzeitig den Anschein erweckte, als sei es legitim. Diese Plattformen umgehen Apples Sicherheitsprüfung, indem sie Apps mit Unternehmenszertifikaten neu signieren, und die Funktion „Benutzerdefinierte Quelle“ von Flekst0re ermöglicht es Nutzern, nicht verifizierte Apps herunterzuladen, die Spyware oder Malware enthalten könnten.

Die Stores von Drittanbietern sind zwar bequem und bieten Zugang zu modifizierten Apps, untergraben aber grundsätzlich die iOS-Sicherheitsvorkehrungen. Dadurch steigt für alle, die sensible Apps wie Banking, Messaging oder E-Mail nutzen, das Risiko.

jamf

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