Security 360:
Jährlicher Sicherheitsreport

Der jährliche Sicherheitsreport von Jamf befasst sich mit Bedrohungen und deren Auswirkungen auf Unternehmen weltweit. Er gibt praktische Tipps für die Konfiguration von Unternehmenstools. User profitieren dadurch auch in 2022 von einer schnellen und sicheren Konnektivität.

Wichtigste Ergebnisse

Die Anzahl der Unternehmen, die eine Malware-Installation auf einem mobilen Gerät verzeichneten, verdoppelte sich von **3 Prozent in 2020 auf 6 Prozent in 2021**.

Im **Jahr 2021 erlaubten 39 Prozent** der Unternehmen den Betrieb von Geräten mit bekannten Betriebssystemschwachstellen in einer Produktionsumgebung ohne Einschränkung der Berechtigungen oder des Datenzugriffs. **28 Prozent waren es noch im Vorjahr.**

7 Prozent der Endgeräte griffen weiterhin auf Cloud-Speicherdienste zu, nachdem sie **in 2021** kompromittiert worden waren.

Im Laufe des Jahres **2021 verdoppelte** sich die Zahl der Geräte, die sich pro Woche mit riskanten Hotspots verbinden, **von 0,5 Prozent auf 1 Prozent**.

1 von 10 Nutzern wird Opfer von Phishing-Angriffen auf Remote-Geräte.

Quelle: Jamf Threat Labs

Einführung

Zu Beginn der weltweiten Pandemie sahen sich Unternehmen mit der schwierigen Aufgabe konfrontiert, die Kontinuität des Geschäftsbetriebs sicherzustellen. Gleichzeitig musste der Übergang zu einer hybriden oder vollständig ferngesteuerten Arbeitsumgebung im Handumdrehen gewährleistet werden. Zwei Jahre später hat sich die Arbeitsumgebung weitgehend auf Remote-Technologien und Cloud-basierte Software umgestellt. So können die Mitarbeiter von praktisch überall aus auf jedem Gerät arbeiten und jederzeit auf Unternehmensdaten zugreifen. Doch wie hat sich dies auf die Sicherheitslage von Unternehmen weltweit ausgewirkt?

Jedes Jahr analysieren wir die Bedrohungen, denen Geräte an modernen Arbeitsplätzen ausgesetzt sind. Mit der zunehmenden Verteilung der Mitarbeiter hat sich auch unsere Sichtweise auf die Bedrohungslandschaft verändert.

Der diesjährige Report befasst sich mit fünf wichtigen Sicherheitstrends. Diese betreffen Unternehmen, deren Nutzer über eine Vielzahl von mobilen Geräten und Plattformen auf zahlreiche Anwendungen zugreifen, die in privaten und öffentlichen Rechenzentren gehostet werden.

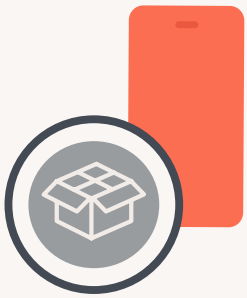
Trend 1 – Anpassung der Sicherheitsstrategie für eine verteilte Belegschaft

Mit der Verlagerung hin zu mehr mobilen Mitarbeitern hat sich auch die Art und Weise verändert, wie IT-Sicherheit umgesetzt wird. Statt traditioneller Lösungen vor Ort, die sich auf den Schutz der Anlagen innerhalb des Büros und des Unternehmensnetzwerks konzentrieren, haben Unternehmen ihre Sicherheitsdienste dezentralisiert. Zudem wurden diese auf die Endgeräte verteilt, die Daten produzieren und verbrauchen, sowie auf Cloud-Anwendungen, die Daten speichern und nutzen. Dies führt zu einer leistungsfähigeren und autarken Sicherheit von Endgeräten sowie zu einer widerstandsfähigeren und robusteren Anwendungssicherheit.

Technologien für den Fernzugriff, die die verteilten Endpunkte und die in der Cloud gehosteten Anwendungen miteinander verbinden, können den Zugriff auf intelligente Weise pro Gerät und pro Anwendung erlauben oder verweigern. Ein Teil dieses Prozesses ist die Entscheidung darüber, welche Indikatoren den Zugriff auf Unternehmensanwendungen verweigern. Schließlich sind Indikatoren für Risiko und Kompromittierung subjektiv.

Hat ein Unternehmen eine hohe Risikotoleranz, benötigt es Indikatoren für die Kompromittierung von Geräten, bevor eine Verbindung zu einer Unternehmensanwendung verweigert wird. Während Indikatoren für die Kompromittierung subjektiv sind, gehören zu den Standardindikatoren von Jamf Threat Labs: (1) Installation von Malware und (2) ein jailbroken oder gerootetes Gerät. Den Daten von Jamf Threat Labs zufolge sind kompromittierte Geräte zwar relativ selten, haben aber dennoch Auswirkungen auf Benutzer und Unternehmen.

2021 verzeichneten 6 Prozent der Unternehmen eine Malware-Installation auf einem mobilen Gerät - doppelt so viele wie in **2020 (3 Prozent)**.



Weniger als 1 Prozent der Organisationen hatten 2021 ein jailbroken oder gerootetes Gerät im Einsatz.

Die beiden oben genannten Ergebnisse lassen den Schluss zu, dass Nutzer ihre Geräte selten manipulieren. Gleichzeitig nehmen die Angriffe auf Unternehmensgeräte stark zu.

Quelle: Jamf Threat Labs

Unternehmen mit einer geringeren Risikotoleranz sollten den Zugriff verweigern, wenn ein Risikoindikator für eine Sicherheitslücke oder eine Gefährdung vorliegt. Die Indikatoren für Sicherheitslücken sind zwar auch subjektiv, aber zu den Standardindikatoren für gefährdete Geräte von Jamf Threat Labs gehören: (1) anfälliges Betriebssystem, (2) Vorhandensein einer unerwünschten Anwendung, (3) Vorliegen eines Drittanbieter-App-Stores und (4) andere Verstöße gegen die Gerätekonformität und Fehlkonfigurationen.

Diese Risikoindikatoren waren auch im Jahr 2021 in unseren Daten enthalten:

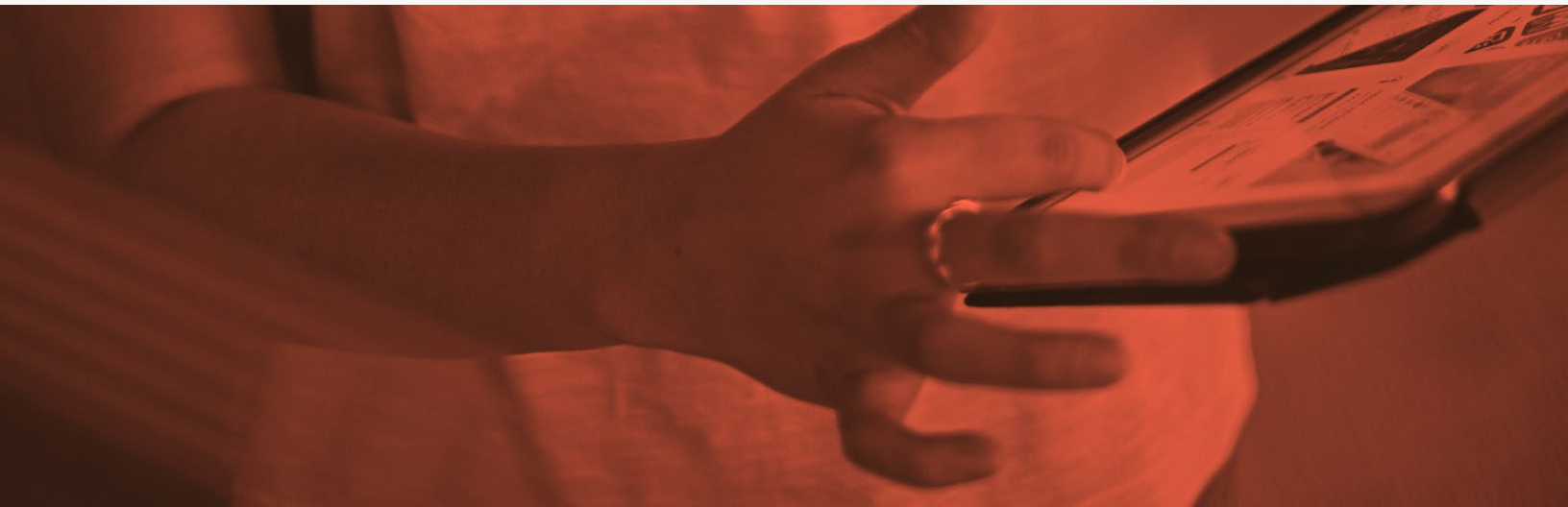
In 39 Prozent der Unternehmen wurde im vergangenen Jahr 2021 regelmäßig ein Betriebssystem mit einer bekannten Sicherheitslücke verwendet, gegenüber **28 Prozent im Vorjahr.**

Im Laufe der Jahres 2021 hat sich die Zahl der Unternehmen, die eine potenziell unerwünschte Anwendung in ihrer Geräteflotte installiert haben, von **5 Prozent auf 11 Prozent mehr als verdoppelt.**

Die Zahl der Geräte, auf denen ein App-Store eines Drittanbieters installiert war, stieg im Laufe des Jahres 2021 von **1 Prozent auf 4 Prozent.**

In 2021 waren **5 Prozent der Geräte bzw. 20 Prozent der Unternehmen** von riskanten Gerätekonfigurationen betroffen.

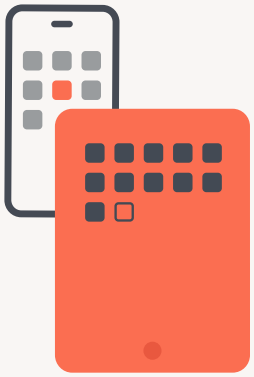
Dies bezieht sich auf jede Anwendung, die nicht nachweislich bösartig ist, birgt aber die Gefahr, dass der Benutzer die Richtlinien umgeht oder unangemessene Inhalte einführt (z.B. über bösartige Werbenetzwerke).



Auch wenn der Prozentsatz der gefährdeten oder anfälligen Geräte gering ist, ist es doch alarmierend, wie viele dieser Geräte auf sensible Daten zugreifen.

7 Prozent der kompromittierten Geräte griffen **im Jahr 2021** auf Cloud-Speicherdienste (wie OneDrive, Google Drive und DropBox) und **25 Prozent** auf E-Mail-Dienste (wie Gmail und Outlook) zu. Diese Zahlen steigen auf **9 Prozent** bzw. **48 Prozent**, wenn die oben genannten Indikatoren für gefährdete Geräte berücksichtigt werden.

9 Prozent der kompromittierten Geräte griffen **im Jahr 2021** auf ein CRM (wie Salesforce und Microsoft Dynamics) und **34 Prozent** auf Konferenzdienste (wie Zoom, Skype und Microsoft Teams) zu. Diese Zahlen erhöhen sich auf **15 Prozent** bzw. **64 Prozent**, wenn die oben genannten Indikatoren für gefährdete Geräte einbezogen werden.



Es macht jedoch keinen Sinn, eine Sicherheitsrichtlinie für den Remote-Zugang auf Grundlage der oben genannten Daten zu definieren, ohne über die erforderlichen Tools zu verfügen, um Risiken zu bewerten und Zugriffsentscheidungen in Echtzeit durchzusetzen. Herkömmliche Fernzugriffstechnologien wie VPN sind sicherlich nicht ausreichend.

Die weltweite Verbreitung der VPN-Technologie, die zur Verschlüsselung des Datenverkehrs über ungesicherte Kommunikationsleitungen verwendet wird, nahm im vergangenen Jahr zu, obwohl in 2020 die Verlagerung zu Cloud-basierten Anwendungen dieses Wachstum verlangsamte. 2021 gaben 43 Prozent der Nutzer im Rahmen einer von security.org durchgeführten Umfrage zu: "Ich kenne es, aber ich benutze es nicht".

Das ist passabel für eine Sicherheitstechnologie, die vor über fünfundzwanzig Jahren entwickelt wurde. Zwar ist die Verwendung von VPN besser als gar kein Schutz. Dennoch haben die Einschränkungen von VPN in Verbindung mit der Tatsache, dass sich die IT-Welt in den letzten Jahren stark verändert hat, zu moderneren Ansätzen für den Fernzugriff geführt, wie Zero Trust Network Access (ZTNA). Dabei handelt es sich um eine Reihe von Sicherheitstechnologien, die einen dynamischen Schutz bieten. Dies wird den Anforderungen neuer Netzwerktechnologien wie Wi-Fi und Mobilfunk gerecht, wobei die vielen Annahmen, auf denen VPN beruht, gebrochen werden. Die Technologie verdankt ihren Namen dem Umstand, dass sie im Gegensatz zu VPN niemals einem Benutzer oder einem Gerät von Natur aus vertraut. Stattdessen lässt ZTNA Verbindungen zu Anwendungen und Diensten erst zu, nachdem überprüft wurde, ob das Gerät und der Benutzer Zugang zu den angeforderten Diensten haben und die Mindestanforderungen für einen sicheren Betrieb erfüllen.

ZTNA wurde mit Blick auf moderne Netzwerke und Arbeitsabläufe entwickelt und lässt sich mit Cloud-basierten Identitätsanbietern (IdP) integrieren. So lassen sich Berechtigungen auf der Grundlage expliziter Benutzerzugriffsrechte verwenden. Datenschutzbewusste ZTNA-Lösungen schützen Daten vor Risiken. Gleichzeitig sind sie flexibel genug, um persönliche Apps und Daten zu schützen und die Privatsphäre der Nutzer zu wahren. Autorisierte Benutzer können sich nur mit den Anwendungen verbinden, für die sie eine Zugriffsberechtigung haben. Dies verhindert, dass Angreifer auf alle Anwendungen im Katalog zugreifen können.

Trend 2 – Angreifer haben ihre Tools und Kampagnen umgestellt: Sie nutzen die Geräte, mit denen User arbeiten

Unternehmen setzen neue Technologien ein, um ihre Kommunikation zu sichern und die Geschäftskontinuität angesichts sich ständig weiterentwickelnder Prozesse aufrechtzuerhalten. Daher haben Bedrohungsakteure ihre Angriffsmethoden und -ziele verbessert, um ihre Wirksamkeit zu erhöhen.

Die Angriffskategorien sind dieselben geblieben, aber die Angreifer haben die Art und Weise der Ausführung erweitert. Dies trägt der Tatsache Rechnung, dass die User jetzt außerhalb traditioneller Büros und auf nutzerfreundlicheren Geräten wie Smartphones, Tablets und Laptops arbeiten. Zudem entscheiden sie sich zunehmend für Apple-Geräte. **Einer kürzlich durchgeführten Umfrage** zufolge würden fast 90% der Arbeitnehmer eine Gehaltskürzung in Kauf nehmen, um die von ihnen bevorzugte Plattform zu nutzen. 62% würden Apple wählen, wenn sie die Möglichkeit dazu hätten.

Während die Zahl der bestätigten Malware-Infektionen nach wie vor gering ist, ist bösartiger Netzwerkverkehr weitaus häufiger. Dieser bezieht sich auf netzwerkbasierte Indikatoren für eine Gefährdung (Indicators of Compromise, IoCs), die in den Kommunikationsmustern zwischen dem Gerät und Internet-Servern beobachtet wird; zu diesen Signalen können Datenexfiltration oder Verbindungen zu Command-and-Control-Servern oder Websites gehören, die bekanntermaßen Malware beherbergen.

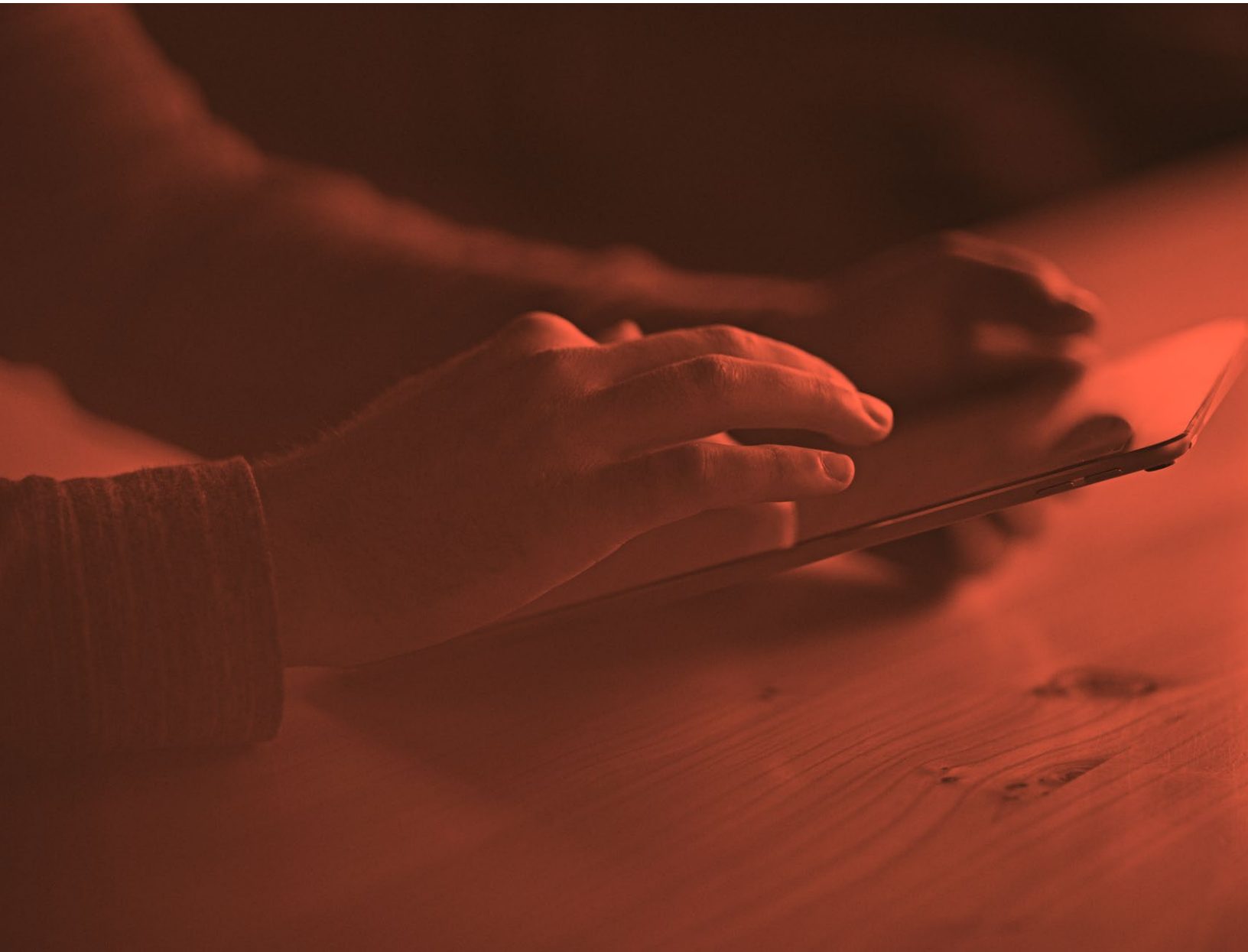
36 Prozent der Unternehmen stießen in **2021** auf Indikatoren für bösartigen Netzwerkverkehr auf einem mobilen Gerät.

Quelle: Jamf Threat Labs

Bösartiger Netzwerkverkehr wird in der Regel nur in Produktionsumgebungen beobachtet und kann nicht einfach durch die Bewertung von statischem Code identifiziert werden. Deshalb ist die Überwachung dieses Indikators über die offiziellen Sicherheitsprüfungen im App Store hinaus so wichtig.

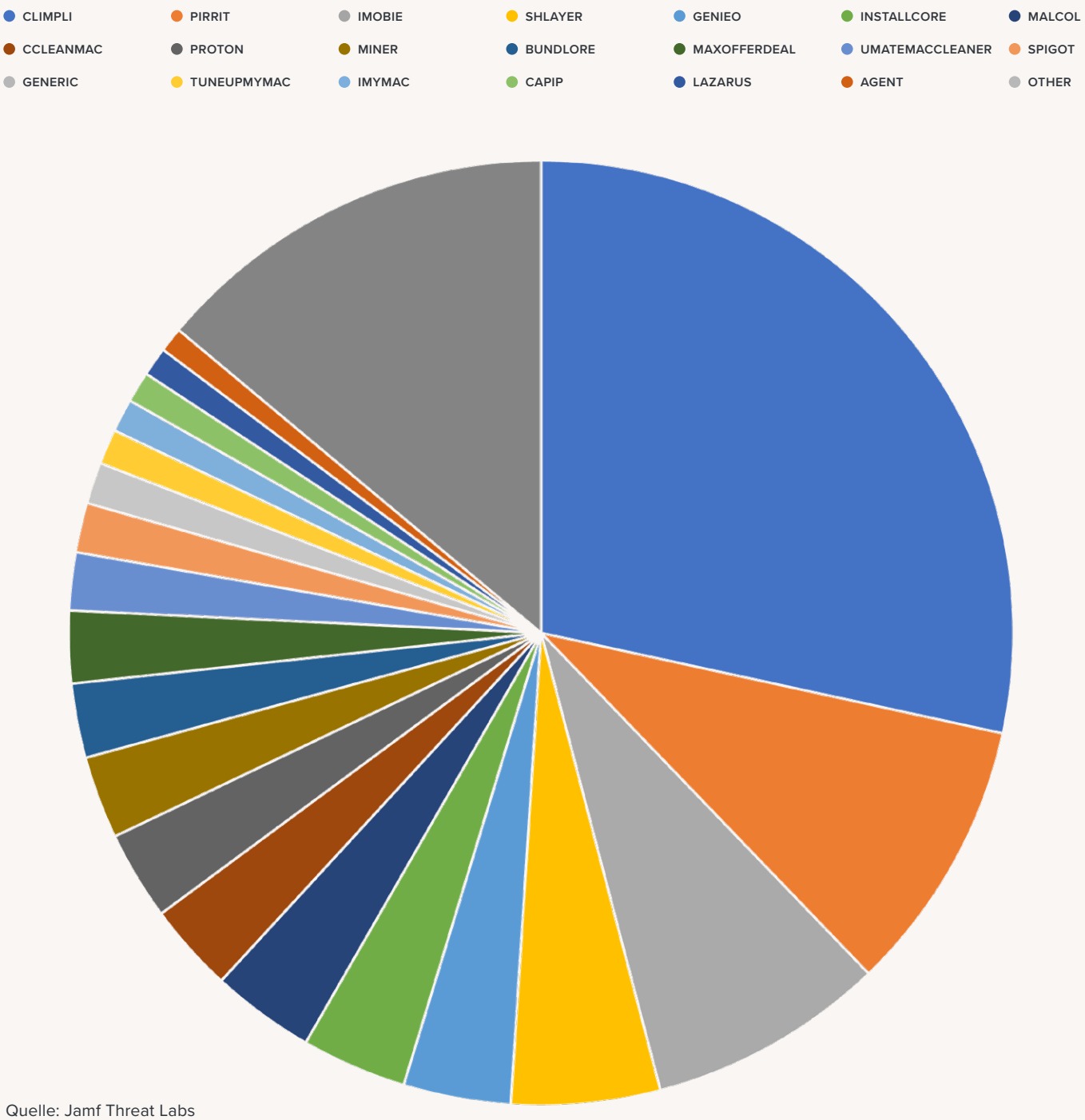
Mac-Malware wird zu einem Problem. 2021 gab Jamf Threat Labs die Entdeckung einer neuen Variante der **Shlayer-Malware** bekannt, mit der Angreifer Gatekeeper, Notarisierung und Datei-Quarantäne-Sicherheitstechnologien in macOS umgehen können. Die Schwachstelle ermöglicht die Ausführung nicht zugelassener Software auf dem Mac und wird über kompromittierte Websites oder infizierte Suchmaschinenergebnisse verbreitet.

Außerdem entdeckte Jamf Threat Labs in 2021 eine **Zero-Day TCC-Umgehung in XCSSET-Malware**. Damit kann ein Angreifer den TCC-Schutz von Apple umgehen, der die Privatsphäre der Benutzer schützt. Die Malware verwendet eine installierte Anwendung mit den richtigen Berechtigungen. Dies kann der Angreifer nutzen, um eine bösartige Anwendung zu erstellen, die auf den Geräten der Opfer ausgeführt wird. Dabei fehlt die Zustimmung des Benutzers für den Zugriff auf Hardware-Funktionen, wie z.B. Kamera oder Mikrofon.



Viele Menschen wissen nicht, dass moderne Mac-Geräte von Malware befallen sind. **Das folgende Diagramm zeigt den Anteil der Mac-Malware-Familien, die im Jahr 2021 versuchten, durch Jamf geschützte Geräte zu kompromittieren.** Die Top 5 waren Climpli, Pirrit, Imobie, Shlayer und Genieo.

Anteil der Mac-Malware-Familien, die in 2021 entdeckt wurden:



Quelle: Jamf Threat Labs

Die Zunahme der Arbeit im Homeoffice und von unterwegs hat zu Sicherheitsbedrohungen geführt, die nicht nur auf Geräte und Anwendungen abzielen, sondern auch auf die Benutzer selbst. Die Bedrohungsakteure haben ihre Phishing-Kampagnen auf moderne Cloud-Anwendungen ausgerichtet, die für die Arbeit genutzt werden, wie Office 365 und Google Workplace (früher G Suite). Da Unternehmen ihre Ressourcen zunehmend in die Cloud verlagern, ist dies ein großes Problem. Ein einziger Fehler eines Mitarbeiters, der einen geschickten Phishing-Angriff erhält (z.B. die Aufforderung, seine Box-Anmeldedaten zu bestätigen), kann einem böswilligen Akteur Zugang zu Unternehmensressourcen verschaffen, die in Cloud-Anwendungen gespeichert sind.

Die Studie von Jamf: **Phishing Trends Report 2021**, die im vierten Quartal veröffentlicht wurde, identifiziert die drei wichtigsten Marken, die bei Phishing-Angriffen Nutzer dazu bringen, sensible Daten preiszugeben. Hierbei entfielen auf Apple, PayPal und Amazon 43 Prozent, 27 Prozent bzw. 9 Prozent dieser Angriffe. Sie erreichten Geräte mit verschiedenen Betriebssystemen und nicht nur Apple-Geräte, obwohl die Marke Apple bei den Angriffen am häufigsten verwendet wurde. Zu betonen ist, dass diese Marken keine Schuld trifft. Sie werden von den Angreifern einfach nur wegen des bekannten Namens benutzt.

Weitere Überlegungen, die sich auf den mobilen Bereich auswirken, sind ein deutlicher Anstieg von Smishing- oder SMS-basierten Phishing-Angriffen, bei denen Benutzer bösartige SMS-Nachrichten von gefälschten Absendern erhalten.

Der Schwerpunkt der Angriffe reicht von E-Mails über Bankgeschäfte und soziale Medien bis hin zu Versuchen, Nutzer zur Preisgabe legitimer Zwei-Faktor-Authentifizierungscodes zu verleiten. Diese haben sie von tatsächlichen Diensten erhalten, um ihre Reichweite auf Bereiche auszudehnen, die mit einer Mehr-Faktor-Authentifizierungstechnologie gesichert sind. Aufgrund der kleineren Bildschirmgröße, der versteckten URL-Leisten, des inhärenten Vertrauens in das Gerät und die Anwendungen sowie der Hektik und Ablenkung bei der Nutzung von Mobiltelefonen sind die Benutzer wahrscheinlich anfälliger für Phishing. Den Daten von Jamf Threat Labs zufolge wird 1 von 10 Nutzern Opfer von Phishing-Angriffen auf dem Handy.

Phishing Trends Report 2021

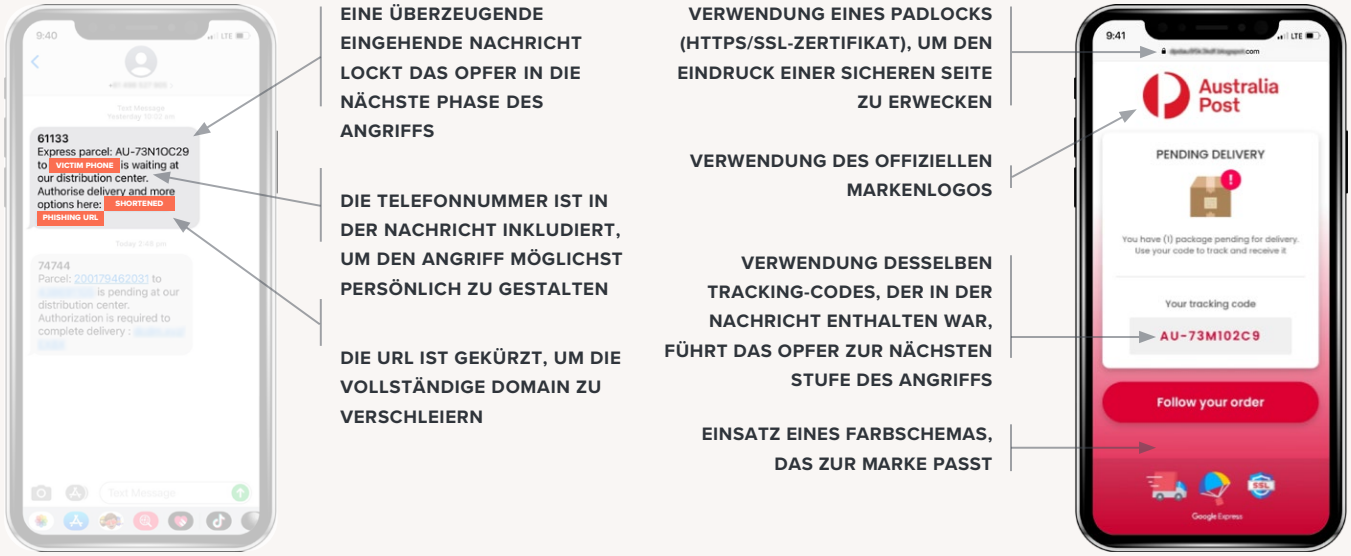
Die 10 meistgenutzten Marken bei Phishing-Kampagnen in 2021

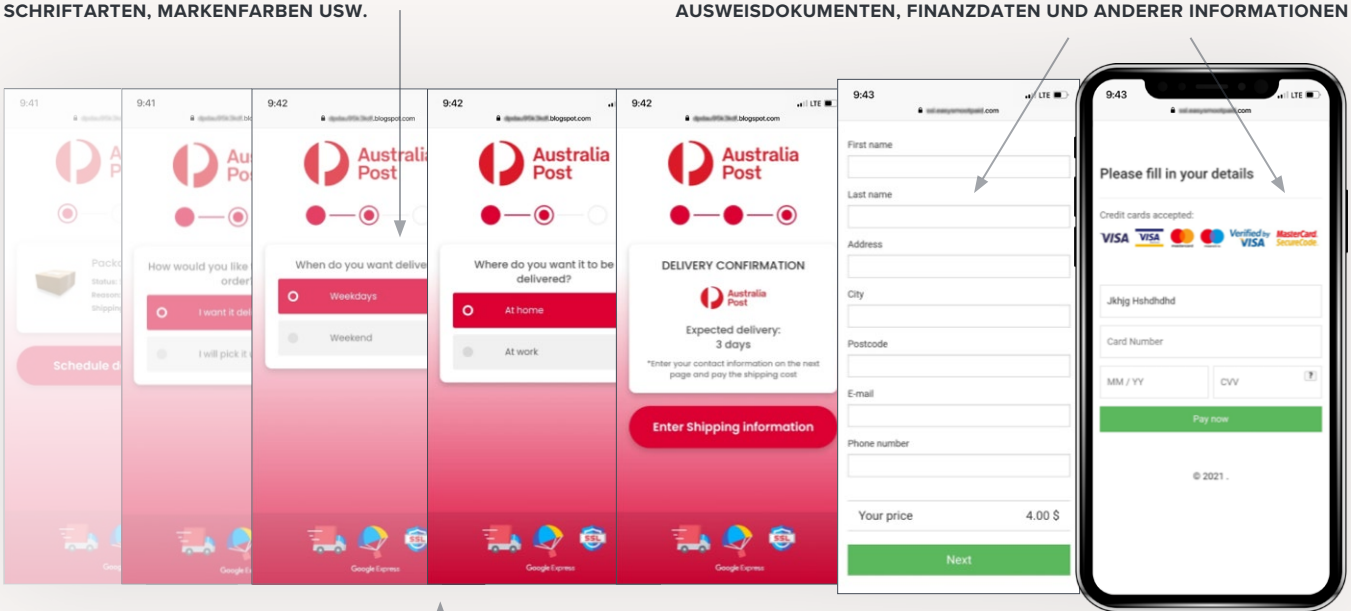
1. **Apple**
2. **PayPal**
3. **Amazon**
4. **Chase**
5. **Facebook**
6. **Google**
7. **Twitter**
8. **Netflix**
9. **Microsoft**
10. **Wells Fargo**

Quelle: Phishing Trends Report 2021 von Jamf

Jamf Threat Labs untersuchte eine Phishing-Kampagne, die auf mobile Geräte ausgerichtet war und bei der mehrere verdächtige Textnachrichten identifiziert wurden. Diese verfolgten eine ähnliche Taktik und fragten dieselben sensiblen personenbezogenen Daten von den Benutzern ab. In den Nachrichten ging es um die Zustellung von Paketen durch die bekannte Australia Post.

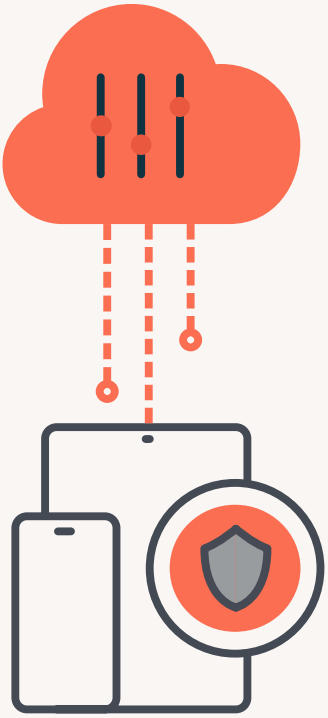
Australia Post ist das Äquivalent von UPS in den USA oder der Deutschen Post in Deutschland, was bedeutet, dass alle in Australien lebenden Postempfänger zu den potenziellen Opfern zählen. Ein opportunistischer Angriff, wenn man bedenkt, wie sehr sich die Menschen während der strengen und wiederholten COVID-19-Lockdowns in Australien auf die Hauszustellung verlassen haben. Wie die anderen großen Marken, die für Phishing-Angriffe missbraucht werden, trifft Australia Post keine Schuld. Die Marke wird von den Angreifern lediglich aufgrund des bekannten Namens verwendet.





Quelle: Jamf Threat Labs

Trend 3 — Das Gleichgewicht zwischen den Sicherheitsanforderungen und der Wahrung der Privatsphäre der Nutzer ist von größter Bedeutung



Schätzungen von Ericsson und der Radicati Group zufolge wird in 2022 die Zahl der Nutzer mit Zugang zur Mobiltechnologie bei 7,26 Milliarden liegen – das sind **etwa 89,76 Prozent der Weltbevölkerung**. Mit dem Zugang zu mehreren Kommunikationsnetzen für ultraschnelle Verbindungen, Multi-Core-Hardware und verlängerter Akkulaufzeit verlassen sich immer mehr Nutzer auf mobile Geräte, um nicht nur private, sondern auch berufliche Aufgaben zu erledigen.

Unternehmen setzen auch auf diesen Trend und unterstützen viele Varianten des Gerätebesitzes, darunter BYOD (Bring Your Own Device), CYOD (Choose Your Own Device), COPE (Corporate Owned, Personally Enabled) und COBO (Corporate Owned, Business Only). So werden die Bedürfnisse des Unternehmens und seiner Nutzer, sei es durch Kostenverlagerung, Produktivitätssteigerung oder Wahlmöglichkeiten für die Mitarbeiter adressiert.

Während sich die IT- und Sicherheitsteams mit sicherheitsrelevanten Prozessen und Arbeitsabläufen befassen, geht es den Endnutzern um ihre Privatsphäre und Autonomie. Genauer gesagt: Wie viel von ihrer Online-Nutzung ist für den Arbeitgeber sichtbar, und wie wird die Nutzung ihrer Geräte durch Sicherheits- und Verwaltungstools beeinflusst?

Während die Sicherheit von größter Wichtigkeit ist, darf die Bedeutung des Datenschutzes nicht unterschätzt werden - vor allem, wenn den Nutzern Firmengeräte zur Verfügung gestellt werden (oder sie ihre eigenen, persönlichen Geräte benutzen). Es kommt die Frage auf: Stellt das Recht auf Privatsphäre die Sicherheitsbedenken in den Schatten oder sind die Anforderungen an die Sicherheitsprozesse wichtiger als die Datenschutzbedenken?

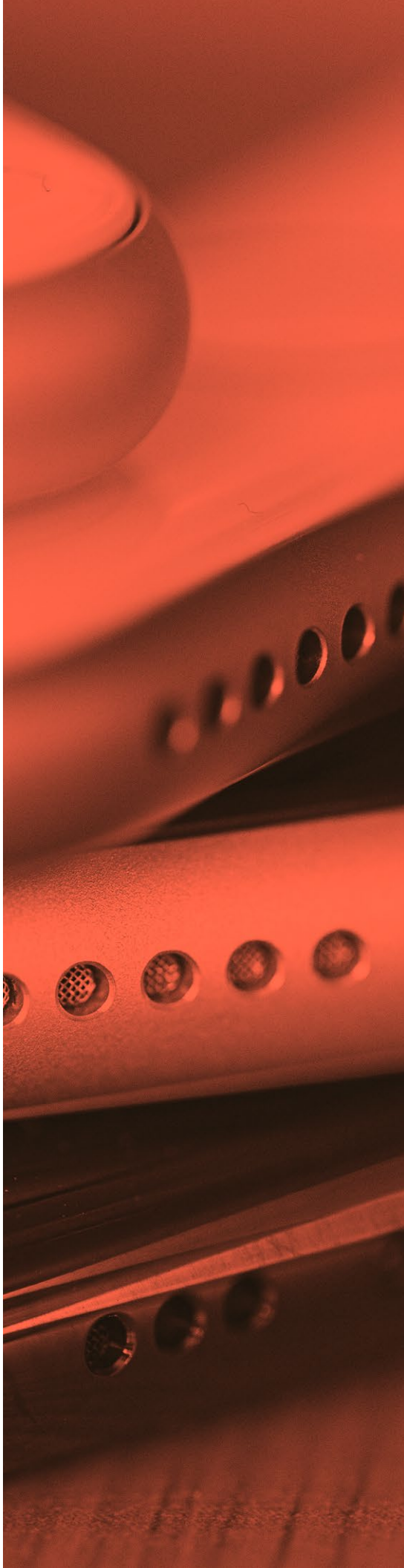
Die Antwort ist nicht ganz eindeutig und hängt stark von der Umgebung und anderen mildernden Faktoren ab, z.B. von gesetzlichen Vorschriften und davon, wer letztlich Eigentümer der Hardware ist. Vor diesem Hintergrund ist Apple führend, indem es Rahmenbedingungen für die auf seinen Geräten ausgeführten Apps bereitstellt. Dies schützt das Recht auf Privatsphäre der Nutzer. Apple hat vor kurzem neue Datenschutz-kontrollen in macOS Mojave eingeführt. Diese machen es erforderlich, dass die Nutzer den Zugriff auf Kameras und Mikrofone, Standort-informationen und Netzwerkverbindungen usw. manuell aktivieren. So werden jetzt Apps und Dienste, die diese Funktionen nutzen, standard-mäßig mit deaktiviertem Zugriff installiert, um die Endnutzer vor unbefugter Überwachung zu schützen.

Aufdringliches Gerätemanagement und Sicherheitslösungen sind nicht die einzigen Datenschutzprobleme, mit denen sich Nutzer konfrontiert sehen. Auch App-Entwickler können in die Privatsphäre der User eingreifen. Vor allem kostenlose Apps machen häufig Nutzerdaten zu Geld.

Laut der Studie von Jamf: **An Analysis of iOS App Permissions**, die im zweiten Quartal veröffentlicht wurde, ist in 2021 die am häufigsten angeforderte Berechtigung der Zugriff auf die Fotobibliothek. 66 Prozent der iOS-Apps, die in unsere Studie einbezogen wurden, forderten diesen Zugriff, gefolgt von Kamera (60 Prozent), Standort (58 Prozent) und Mikrofon (34 Prozent). Und es gab eine ganze Reihe von verdächtigen App-Kategorien, die Zugriffsrechte beantragten, die sie nicht benötigen. So ist es zum Beispiel logisch, dass die Mehrheit (62 Prozent) der Navigations-Apps Zugriff auf den Standort verlangt. Aber warum erfordert fast die Hälfte (48 Prozent) auch Zugriff auf die Kamera?

Das Gleiche gilt für 83 Prozent der Shopping-Apps, die Zugriff auf die Kamera verlangen. Für das Scannen von QR-Codes ist das sinnvoll, aber warum erfordern so viele (87 Prozent) auch Zugriff auf die Fotobibliothek? Nutzer sollten darüber nachdenken, welche Berechtigungen eine App wirklich braucht, bevor sie auf "Akzeptieren" drücken.

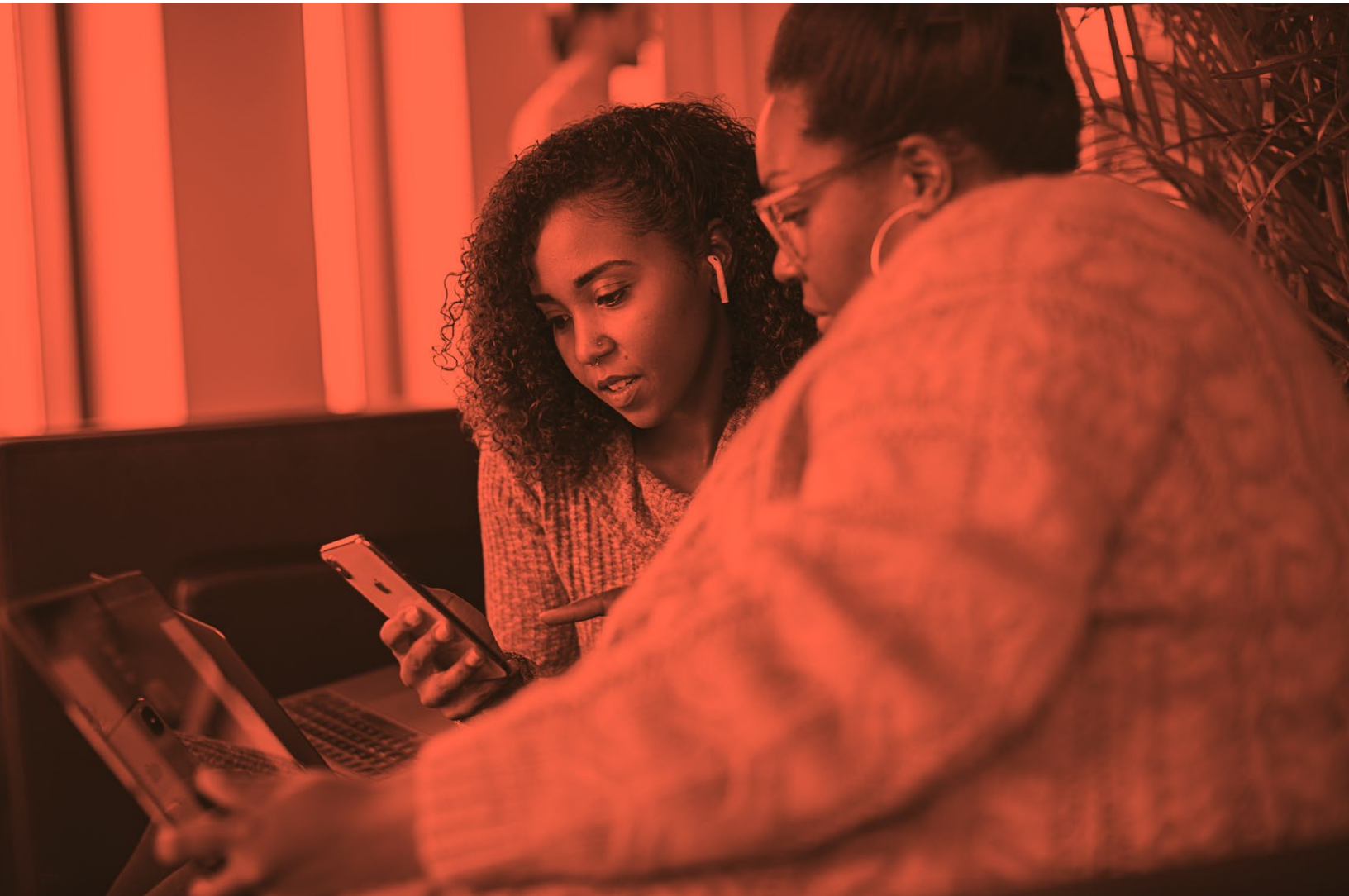
An Analysis of iOS App Permissions



Doch was passiert, wenn der Zugang einmal gewährt ist? Wie kann dann das Data Mining von persönlichen Informationen eingedämmt werden? An dieser Stelle kommen Apples App-Tracking-Transparency-Framework und Googles Werbe-ID-Richtlinie ins Spiel, um die unbefugte Weitergabe von Daten zu verhindern. Beide Lösungen setzen voraus, dass die Entwickler sie bei der Programmierung ihrer Anwendungen und Dienste verwenden, wodurch die Kontrolle über die Daten direkt in die Hände der Nutzer gelegt wird.

Darüber hinaus erfüllen Device-Management-Lösungen wie Jamf Pro diese Anforderungen. Die IT-Abteilung kann damit Unternehmens-Apps benennen, die nicht nur bereitgestellt, sondern auch sicher verwaltet werden können. Dabei können sie nicht auf persönliche Apps - oder deren Daten - auf persönlichen Geräten, die Teil eines BYOD-Modells sind, oder auf unternehmenseigenen Geräten, die Teil eines CYOD/COPE-Modells sind, zugreifen oder mit ihnen interagieren.

Sie stellen ein Gleichgewicht zwischen der Sicherung von Apps und Daten sowie des Geräts selbst her, überlassen aber den Nutzern die Kontrolle über die privaten Daten im Zusammenhang mit ihren persönlichen Apps und der Nutzung des Geräts. So können Unternehmen geschützte Daten, die sowohl sensibel als auch vertraulich sind, am besten schützen. Gleichzeitig behalten sie einen "Hands-off"-Ansatz für persönliche Nutzerdaten bei, mit denen Endnutzer den Grad des Zugriffs auf diese Daten kontrollieren können. Dadurch wird der Datenschutz insgesamt weiter verbessert.



Trend 4 — Endnutzer sind immer noch die größte Bedrohung für die Datensicherheit

Für die Sicherheit gilt vor allem eines: Unabhängig von der Art der vorhandenen Sicherheitskontrollen, ihrer Konfiguration zur Überwachung, Erkennung und Minderung von Risiken und trotz des Automatisierungsgrads zur Verhinderung und Behebung sicherheitsrelevanter Probleme können all diese Bestrebungen von einem Nutzer unwissentlich rückgängig gemacht werden.

Dies geschieht nicht aus Furcht, Unsicherheit und Zweifel, sondern ist eine reale Wahrheit über das Schutzniveau von Unternehmensnetzwerken. Dabei wird die Schulung der Benutzer oft wenig bis gar nicht berücksichtigt. Das ist der Grund, warum böswillige Akteure bei ihren Versuchen, durch Phishing und unerwünschte Software-Kampagnen an sensible Daten zu gelangen und schließlich in Unternehmensnetzwerke einzudringen, immer wieder auf diese "niedrig hängenden Früchte" abzielen.

Ein Sprichwort besagt, dass die Sicherheit in der Verantwortung aller liegt. Am kontinuierlichen Erfolg von IT-Sicherheit haben alle Beteiligten ihren Anteil, unabhängig von ihrer Rolle innerhalb einer Organisation. Und leider gibt es sehr grundlegende Sicherheitsmaßnahmen, die immer noch übersehen werden. Laut den Daten von Jamf Threat Labs war bei 2 Prozent der für die Arbeit genutzten Geräte die Bildschirmsperre deaktiviert, gegenüber 3 Prozent im Vorjahr. Dies stellt eine erhebliche Gefahr dar, wenn ein Firmengerät verloren geht oder gestolen wird.

Laut dem **Internet Crime Report 2020 des FBI**, der im Jahr 2021 veröffentlicht wurde, waren in 2021 die drei häufigsten von den Opfern gemeldeten Straftaten (1) Phishing-Betrug, (2) Betrügereien wegen Nichtzahlung/Lieferverweigerung und (3) Erpressung. Dieser Bericht hebt auch hervor, dass 2020 über 240.000 Menschen Opfer von Phishing-Angriffen (einschließlich Vishing, Smishing und Pharming) wurden, mehr als doppelt so viele wie im Vorjahr und mit einem Schaden von mehr als 54 Milliarden Dollar. Außerdem waren mehr als doppelt so viele Menschen von Phishing betroffen wie von der zweitgrößten Straftat: Nichtzahlung/Nichtlieferung. Die Folgen von Phishing für Verbraucher sind schlimm genug, aber die Auswirkungen auf Unternehmen sind noch gravierender. **Laut dem Data Breach Investigations Report 2021 von Verizon waren 36 Prozent der Datenschutzverletzungen auf Phishing zurückzuführen, 11 Prozent mehr als im Vorjahr.**

2 Prozent der beruflich genutzten Geräte hatten im Jahr 2021 die Bildschirmsperre deaktiviert, **gegenüber 3 Prozent im Vorjahr.**

Laut den Daten von Jamf Threat Labs ist in **einem Drittel (29 Prozent)** der Unternehmen in **2021** mindestens ein Benutzer auf einen Phishing-Angriff hereingefallen.

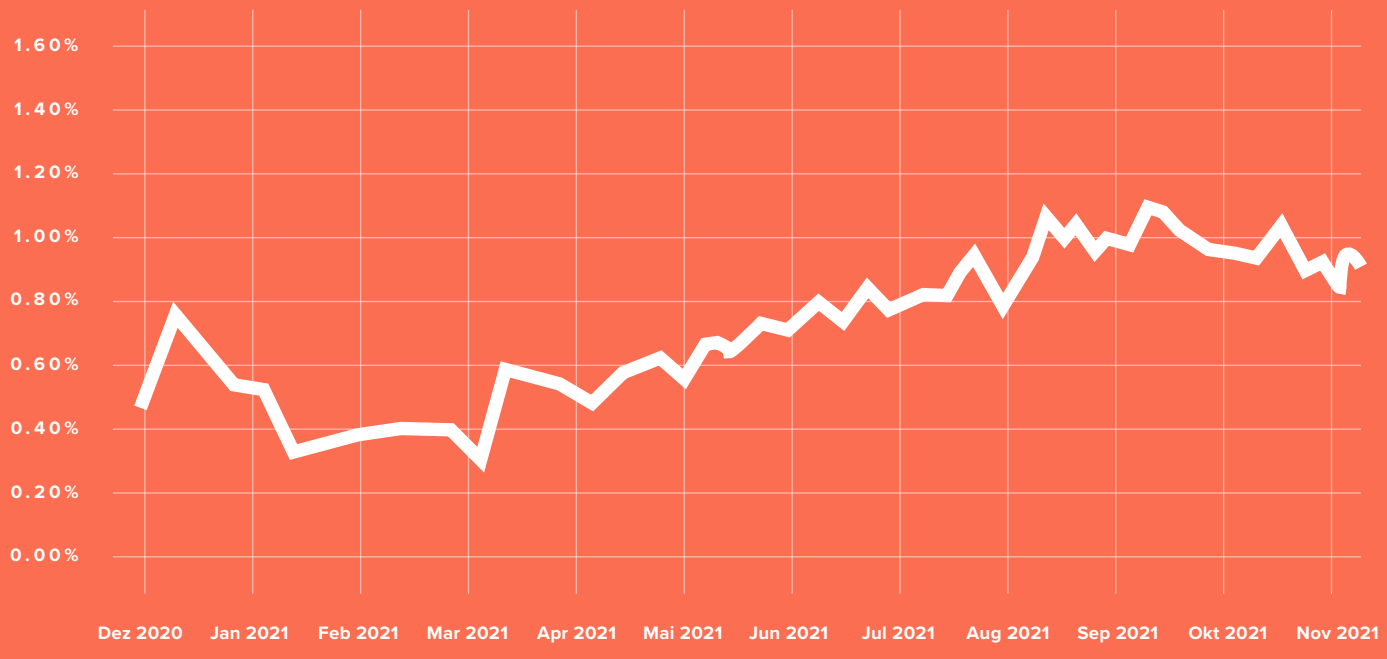
Quelle: Jamf Threat Labs

Die Nutzer können sich auch unterwegs mit riskanten Hotspots verbinden. Die Bequemlichkeit des kostenlosen Wi-Fi am Flughafen oder im Café ist oft zu verlockend für Mitarbeiter, die sich keine Gedanken über die potenziellen Auswirkungen eines Angriffs machen. Hierbei nutzt ein bösartiger Akteur eine Wi-Fi-Verbindung, um unbemerkt eine Datenübertragung abzufangen, ein so genannter Man-in-the-Middle-Angriff (MitM). Aber das sind nicht die einzigen Risiken, die von Wi-Fi ausgehen. Es gibt eine Reihe von Indikatoren für einen riskanten Hotspot, die Daten gefährden können. Dazu zählt ein verdächtiges Root-Zertifikat eines Drittanbieters, das die Authentizität vertrauenswürdiger SSL-Verbindungen durch das Abfangen verschlüsselter Kommunikation gefährden könnte.

Im Laufe des Jahres 2021 verdoppelte sich die Anzahl der Geräte, die pro Woche eine Verbindung zu riskanten Hotspots herstellten, **von 0,5 Prozent auf 1 Prozent.** Dies ist möglicherweise auf vermehrtes Reisen und Pendeln zurückzuführen, da die Pandemiebeschränkungen gelockert wurden.

Quelle: Jamf Threat Labs

Geräte, die pro Woche eine Verbindung zu riskanten Hotspots herstellen



Quelle: Jamf Threat Labs

Geräte, die pro Woche eine Verbindung zu riskanten Hotspots herstellen

Die Investition in Schulungsprogramme für das Sicherheitsbewusstsein der Mitarbeiter ist ein wichtiger Bestandteil der Sicherheitsstrategie eines Unternehmens und sollte nicht vernachlässigt werden. Dies bedeutet, dass fortlaufende Schulungen für Endbenutzer durchgeführt werden müssen. Diese sollten eine Vielzahl von bewährten Verfahren abdecken und die Benutzer über die neuesten Bedrohungen aufklären. Dadurch können sie neue Angriffe besser erkennen und aktive Schritte zur Verbesserung ihrer Sicherheitshygiene unternehmen — und zwar nicht nur bei der Arbeit, sondern auch im Privatleben.

Trend 5 — Das Management von App-Risiken wird immer komplexer

Apps sind das Lebenselixier der Computerwelt. Da die Nutzung von Apps von der Internetverbindung abhängt, bieten Cloud-basierte Apps und Dienste den Nutzern eine Fülle von Optionen. Dadurch können sie produktiv bleiben und Zeiten genießen, in denen sie nicht im Einsatz sind — und das alles von ein und demselben Gerät aus. Doch die Zunahme von Malware in Verbindung mit Angriffen in der Lieferkette kann dazu führen, dass potenziell unerwünschte und bösartige Apps auf Geräten installiert werden. Diese können Daten und sensible Informationen preisgeben und das Gerät und damit das Unternehmen gefährden.

Das Jailbreaking von Geräten, bei dem die internen Sicherheitsvorkehrungen aufgehoben werden, um die Änderung bestimmter Funktionen zu ermöglichen, ist nicht illegal. Der Zugriff auf App-Stores von Drittanbietern, in denen fragwürdige Apps angeboten werden, die normalerweise nicht in den offiziellen App-Stores von Apple und Google erhältlich sind, ist ebenfalls nicht illegal. Allerdings können diese Aktivitäten zur Installation illegaler "gecrackter" Apps führen, die keine Lizenz des Entwicklers haben. Unabhängig von der Legalität ist das Sicherheitsrisiko beim Sideloading von Apps ähnlich hoch wie beim Jailbreaking. In beiden Fällen können riskante Apps installiert werden, die Geräte mit Malware infizieren, Benutzer ausspionieren, persönliche Daten stehlen oder weitergeben, ihr Gerät mit Werbung überfluten oder es komplett lahmlegen. Laut Daten von Jamf Threat Labs hatten 2021 weniger als 1 Prozent der Unternehmen ein oder mehrere jailbroken oder gerootete Geräte in ihrer Flotte und 5 Prozent der Unternehmen hatten 2021 auf einem oder mehreren Geräten eine Drittanbieter-App installiert.

Der interne Code dieser inoffiziellen oder illegal erworbenen Versionen von Anwendungen wird weder überprüft noch auf Sicherheitsbedrohungen gescannt, wie die Anwendungen in den offiziellen App-Stores. Das bedeutet, dass eine Anwendung, die sich als sichere Browser-Alternative ausgibt, in Wirklichkeit Malware sein kann.

Bei der Auswahl von Apps für die genehmigte geschäftliche Nutzung sollten IT-Teams sicherstellen, dass sie für die Verwendung mit der Infrastruktur des Unternehmens ordnungsgemäß geprüft sind. Und sie sollten eine kontinuierliche und dynamische App-Prüfung durchführen, die über eine statische Codeprüfung hinausgeht. Auf diese Weise können Probleme erkannt werden, die auftreten, wenn die App während der Nutzung auf das Internet zugreift. Dazu zählen z.B. schwache oder fehlende Verschlüsselungscodes, Ad-Delivery-Netzwerke, die bekanntermaßen Malware liefern, oder **unbekannte oder nicht angekündigte "Funktionen", die effektiv eine trojaner-ähnliche Situation schaffen**. Darin wird eine App für eine Funktion verwendet, während heimlich eine andere Funktion im Hintergrund läuft.

Weniger als 1 Prozent der Unternehmen hatten **im Jahr 2021** ein oder mehrere jailbroken oder gerootete Geräte in ihrer Flotte.

Und **5 Prozent** der Unternehmen haben in **2021** auf einem oder mehreren Geräten eine Drittanbieter-App installiert.

Quelle: Jamf Threat Labs

Ein weiteres wichtiges Problem im Zusammenhang mit der App-Sicherheit sind Pipeline-Angriffe oder solche, die darauf abzielen, den Vertriebs- oder Lieferkanal zu kompromittieren. So schädigen sie indirekt alle Geräte, die auf die kompromittierte App oder den Dienst angewiesen sind. Diese Form von Angriffen ist zwar schwer zu erkennen, da sie sich in der Regel gegen den Hersteller oder Entwickler der App selbst richtet. Doch haben sie in der Regel tiefergreifende und länger anhaltende Auswirkungen auf die betroffenen Unternehmen, wie **hier in einem Bericht von CNN über den SolarWinds-Angriff** erläutert wird. Dieser kompromittierte im Dezember 2020 kommerzielle Software zur Verwaltung von Netzwerkgeräten. Organisationen können Vorkehrungen treffen, um sich so weit wie möglich vor dieser Art von Risiken zu schützen.

Wir empfehlen, Anwendungen und Dienste nur von bekannten Entwicklern über die offiziellen App-Stores für das Geräte-Ökosystem bereitzustellen. Das Testen von Anwendungen in nicht produktiven Umgebungen ermöglicht es IT- und Sicherheitsteams, die Funktionsweise der App bzw. des Dienstes einzuschätzen und ermöglicht ihnen, alle erforderlichen Anpassungen vorzunehmen. Unternehmen, die interne Apps entwickeln, sollten sicherstellen, dass ihre Entwicklungsinfrastruktur gesichert ist und der Zugang auf die Personen beschränkt ist, die ihn benötigen. Dazu sollten z.B. Programmierer die Anzahl der in diesen Testumgebungen ausgeführten Apps auf das für die Entwicklung der App erforderliche Maß reduzieren. Die Einhaltung von Praktiken zur sicheren App-Entwicklung, die regelmäßige App-Überprüfung und die ständige Aktualisierung der Umgebungen tragen dazu bei, das Eindringen von Malware in Entwicklungsstandorte zu vermindern und die Wahrscheinlichkeit zu minimieren, dass ein Dritter den Entwicklungs-Workflow kompromittiert.

Empfehlungen

Trotz eines jahrzehntelangen Versuchs, IT-Standards für Unternehmen zu definieren, sind viele Unternehmen an einem Punkt angelangt, an dem der Mangel an Standardisierung zum Standard geworden ist. Laut der **Verizon MSI-Umfrage** gaben im Jahr 2021 fast ein Viertel (24 Prozent) der Befragten an, dass ihr Unternehmen die Sicherheit mobiler Geräte geopfert hat, um auf die Einschränkungen in der Pandemie zu reagieren. Welches Betriebssystem wird in Ihrem Unternehmen verwendet? Alle. Welcher Art von Benutzern erlauben Sie den Zugriff auf Ihre Anwendungen? Allen. Von welchen Standorten aus dürfen die Benutzer arbeiten? Von jedem. Sichere Fernzugriffslösungen müssen so flexibel und beweglich sein, dass sie den Zugriff ermöglichen und nicht blockieren und die Produktivität nicht behindern. Wir empfehlen die Verwendung dieser Checkliste für die Entwicklung einer modernen, cloudbasierten Sicherheitsstrategie, die den Anforderungen der heutigen hybriden IT-Umgebungen entspricht.

Skizzieren Sie die Anforderungen auf Grundlage der neuen Anwendungsfälle, die durch die Fernarbeit entstehen

- Was wollen Sie Ihren Mitarbeitern auf ihren Geräten ermöglichen — den Zugriff auf E-Mails oder auf sensible Datenbanken? Segmentieren Sie Daten, damit der Zugriff granular erfolgen kann.
- Evaluieren Sie Ihre Anwendungsfälle und definieren Sie die Anforderungen für Ihre Remote-Mitarbeiter.
- Die oben genannten Anforderungen bilden die Grundlage für Ihr Geräteeigentumsmodell — welche Gerätetypen werden Sie unterstützen, wem gehören sie, wie werden sie verwaltet?
- Priorisieren Sie die Bedürfnisse der Endbenutzer, um die Akzeptanz von Sicherheitstools zu gewährleisten — wählen Sie Lösungen, die sie nicht behindern oder verlangsamen, und die für das von ihnen verwendete Geräte-Ökosystem geeignet sind.

Schnelle und sichere Konnektivität

- In Bezug auf Konnektivität und Cloud-Anwendungen sollten Sie festlegen, was Sie über Benutzer, Geräte, Netzwerke und Anwendungen wissen müssen, bevor Sie ihnen Zugang zu Unternehmensressourcen gewähren.
- Beschränken Sie die Benutzer auf die von ihnen benötigten Geschäftstools, um zu verhindern, dass privilegierte Konten für Angriffe auf eine große Anzahl von Systemen missbraucht werden.
- Führen Sie einen kontinuierlichen bedingten Zugriff für die Echtzeitbewertung der Richtlinien ein.

Definition und Durchsetzung von Richtlinien zur Nutzung

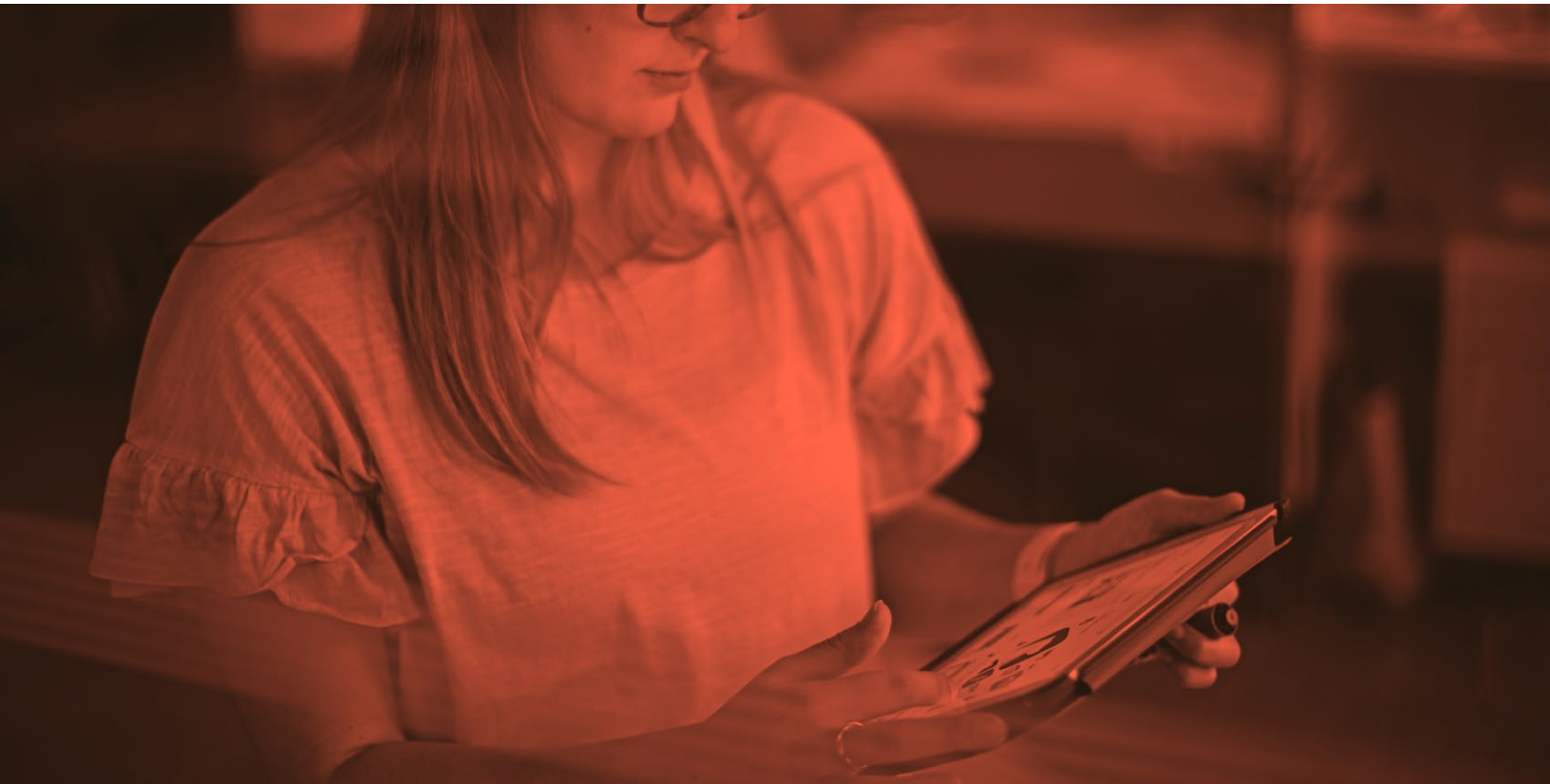
- Überprüfen Sie Ihre bestehenden Richtlinien zur Nutzung und stellen Sie sicher, dass alle Arten von Endgeräten berücksichtigt werden.
- Implementieren Sie eine Richtlinie zur Nutzung für jede geeignete Untergruppe von Geräten, um Schatten-IT und unerwünschte Nutzung zu kontrollieren und die Einhaltung von Vorschriften zu gewährleisten.

Bereitstellung einer flexiblen Verwaltungslösung, die sich an alle Gerätebesitzmodelle anpasst

- Setzen Sie eine Verwaltungslösung ein, mit der Sie Geräte mit Unternehmensressourcen versorgen, Konten und Konnektivität konfigurieren und laufende Sicherheits- und Konformitätsprüfungen durchführen können, ohne dass es zu einer Überverwaltung kommt und die Privatsphäre der Benutzer beeinträchtigt wird.
- Richten Sie automatisierte Maßnahmen für Geräte ein, die nicht konform sind oder sich in einem anfälligen oder gefährdeten Zustand befinden, um sie wieder konform zu machen.

Erweiterung der Zugriffsverwaltungsrichtlinien, um die Risikolage von Geräten zu berücksichtigen

- Implementieren Sie eine benutzerfreundliche IAM-Lösung (Identity and Access Management) für die Authentifizierung bei Unternehmensanwendungen auf allen Geräten, einschließlich Mobilgeräten.
- Integrieren Sie Risikobewertungen für Geräte in Ihre IAM-Richtlinien und stellen Sie sicher, dass die Risikolage der Geräte berücksichtigt wird.
- Stellen Sie sicher, dass die Risikolage während der gesamten Dauer einer Sitzung kontinuierlich bewertet wird.



Eine cloud-basierte Sicherheitslösung ist besonders wichtig für den Schutz vor einem breiten Spektrum von Cyber-Bedrohungen und Nutzungsrisiken, einschließlich Zero-Day-Angriffen.

- Stellen Sie sicher, dass Ihre Sicherheitslösung über eine starke Endpunkt-Erkennungsfunktion mit geräteinternen Funktionen verfügt, die durch netzwerkbasierte Präventionsmaßnahmen ergänzt werden, um Angriffe zu stoppen, bevor sie ein Gerät erreichen.
- Stellen Sie sicher, dass Ihre Sicherheitslösung sowohl externe Cyber-Bedrohungen (wie Phishing, Man-in-the-Middle-Angriffe und Malware) als auch Risiken durch das Nutzungsverhalten abdecken kann.
- Stellen Sie sicher, dass für alle Sicherheitstools geeignete Konfigurationen vorgenommen werden, um die Bedrohungsvektoren für Ihr Unternehmen unter Wahrung der Privatsphäre Ihrer Endnutzer zu identifizieren.
- Bewerten Sie die Fähigkeit der Sicherheitslösung zum maschinellen Lernen. Verstehen Sie dadurch, wie die Engine neue und unbekannte Bedrohungen identifiziert und vor ihnen schützt (Heuristik/Verhaltensanalyse).

Überprüfen Sie diese Liste regelmäßig und überlegen Sie, welche Änderungen aufgrund folgender Punkte vorgenommen werden müssen:

- Änderungen der Unternehmensgröße und -zusammensetzung, z.B. Fusionen oder Übernahmen
- Neue Vorschriften, die sich auf Ihren Umgang mit Daten auswirken
- Weiterentwicklung der IT-Strategie
- Bedrohungen, die Sie bei Mitarbeitern beobachtet haben
- Anschaffung neuer Geräte und Außerbetriebnahme von Geräten am Ende ihres Lebenszyklus
- Neue Anwendungen, die Mitarbeiter für ihre Arbeit benötigen
- Änderungen an Betriebssystemen, die das Management, den Einsatz und den Datenschutz regeln

Über diese Studie

Wir wollten die wichtigsten Sicherheitstrends in der neuen Welt der hybriden Arbeit besser verstehen. Die Informationen und Statistiken in diesem Dokument sind das Ergebnis unserer Analyse innerhalb einer Stichprobe von 500.000 Geräten, die von Jamf geschützt werden, und zwar für iOS, macOS, iPadOS, Android und Windows in 90 verschiedenen Ländern und über einen Zeitraum von 12 Monaten. Diese Analyse wurde im vierten Quartal 2021 durchgeführt.
Die in dieser Untersuchung analysierten Metadaten stammen aus aggregierten Protokollen, die keine persönlichen oder organisations-identifizierenden Informationen enthalten. Mit dieser Analyse wollen wir keine Angst schüren. Stattdessen informieren wir Sie und Ihre Benutzer über die verfügbaren Optionen und darüber, wie Sie alle Aspekte der Geräte-, Benutzer- und Unternehmensdaten am besten schützen können. Setzen Sie sich mit uns in Verbindung und erfahren Sie, wie Sie Schutzmaßnahmen ergreifen und Ihre Sicherheitslage verbessern können.