jamf

Sicherheit 360:
Jährlicher Trendbericht

Einführung

Im vergangenen Jahr haben wir untersucht, wie sich die Einführung von Remote-Technologien auf die Sicherheitslage von Unternehmen weltweit auswirkt. Während viele Unternehmen immer noch auf Remote- und hybride Arbeitsumgebungen umstellen, wird der Schwerpunkt in diesem Jahr darauf liegen, wie sich die Bedrohungslandschaft angepasst hat und wie diese Trends ein Sicherheitsrisiko für Ihr Unternehmen durch bestehende und neu entwickelte Bedrohungen darstellen.

Jedes Jahr analysiert **Jamf Threat Labs** die Bedrohungen, die auf die am modernen Arbeitsplatz verwendeten Geräte einwirken. Da die Belegschaft immer weiter verstreut ist, entwickelt sich unsere Perspektive auf die moderne Bedrohungslandschaft weiter, um die konsistenten Anforderungen der Endpunkt-Compliance zu erfüllen und die Datensicherheit zu gewährleisten, während die Privatsphäre der Benutzer*innen angesichts der sich entwickelnden Risiken gewahrt bleibt.

Der diesjährige Bericht befasst sich mit fünf wichtigen Sicherheitstrends, die sich auf Unternehmen auswirken, deren Benutzer*innen per Fernzugriff auf eine Vielzahl von Apps und Diensten zugreifen, die in privaten und öffentlichen Rechenzentren gehostet werden und sich auf verschiedene plattformübergreifende mobile Geräte verlassen.

2023 Trends Adresse:

1. Social Engineering
2. Privatsphäre der Nutzer*innen
3. Neuartige Bedrohungen
4. Compliance
5. Verteilung der Arbeitskräfte

Trend 1 - Social Engineering ist weiterhin die größte Bedrohung

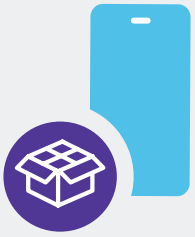
Social Engineering, insbesondere Phishing-Angriffe, stehen ganz oben auf der Liste der größten Bedrohungen für die Cybersicherheit. Die unbeständige Mischung aus verteilten Mitarbeiter*innen und der relativen Leichtigkeit, mit der böswillige Akteure Phishing-Kampagnen durchführen können, führt dazu, dass Benutzeranmeldedaten erfolgreich erlangt werden. Diese Angriffsarten, die auch als „Schlüssel zum Königreich" bezeichnet werden, ermöglichen unbefugten Benutzer*innen den Zugriff auf lokal im Gerät gespeicherte Daten. Was diese Angriffe noch gefährlicher (oder wirkungsvoller) macht, ist die Tatsache, dass sie es ihnen oft ermöglichen, als Teil ihrer Angriffskette auf andere Systeme zuzugreifen.

Die Ironie der Social-Engineering-Angriffe besteht darin, dass viele Lösungen trotz starker Sicherheitskonfigurationen, die den Best Practices der Branche entsprechen, wenig zur Verhinderung dieser Art von Angriffen beitragen können, wenn Benutzer*innen dazu verleitet werden, ihre Anmeldedaten an böswillige Akteur*innen weiterzugeben und sich als jemand auszugeben, der sie nicht sind. Erschwerend kommt hinzu, dass die Umgebungen inzwischen so uneinheitlich sind, dass viele Benutze*innenr keinen einfachen Zugang zu IT- und Sicherheitsexpert*innen haben, wenn sie verdächtige E-Mails oder SMS-Nachrichten erhalten, die scheinbar eine sofortige Reaktion erfordern.

Leider ist es aufgrund des aufkommenden Charakters der Nachrichten – die absichtlich so geschrieben sind, um die Opfer zu erschrecken, damit sie auf einen Link klicken, der ihre Authentifizierungs-Token stiehlt, bösartigen Code ausführt, um eine Schwachstelle auf ihrem Gerät auszunutzen, oder das Opfer einfach auf eine gefälschte Website leitet, die sich als eine legitime ausgibt, um sie zur Angabe ihrer Anmeldedaten zu verleiten - die traurige Tatsache, dass es zu dem Zeitpunkt, an dem der Benutzer*innen mit der IT-Abteilung gesprochen hat, meist schon zu spät ist. So **berichtete IBM**, dass gestohlene oder kompromittierte Zugangsdaten nicht nur die häufigste Ursache für Datenschutzverletzungen waren, sondern mit 327 Tagen auch die längste Zeit zur Identifizierung benötigten.

Phishing-Angriffe unterscheiden sich erheblich von anderen Arten von Angriffen, d. h. es handelt sich nicht um anonyme Akteur*innen, die lügen, um an Ihren Benutzernamen und Ihr Passwort zu gelangen. Die Täuschung kann auf verschiedene Weise erfolgen, um das gleiche Ergebnis zu erzielen: Ein beliebter Angriff, der überall dort durchgeführt wird, wo öffentliche Hotspots (siehe „kostenloses WLAN") verfügbar sind, nennt sich zum Beispiel „evil twin". Ein böser Zwilling tarnt sich als legitimes drahtloses Netzwerk und ermöglicht es einem Angreifer, effektiv alle relevanten Daten zu stehlen, die vom Opfer ohne dessen Wissen übertragen werden. Dies kann vermieden werden, wenn das Gerät, das auf das Netzwerk zugreift, mit einer **VPN- oder Zero Trust Network Access (ZTNA)-Lösung verschlüsselt ist**.

Im Jahr 2022 wurde bei 31 % der Unternehmen mindestens ein Benutzer/ eine Benutzerin Opfer eines **Phishing-Angriffs.**



Im Jahr 2022 wurde festgestellt, dass 16 % der Nutzer*innen sensible Daten preisgeben, indem sie sich mit **riskanten Hotspots verbinden.**

Diese beiden Daten deuten darauf hin:

1. Die Benutzer*innen manipulieren ihre Geräte viel weniger als früher, und...
2. Böswillige Akteur*innen greifen verstärkt Geräte von Unternehmen an.

Quelle: Jamf Threat Labs

Statistica schätzt, dass es derzeit weltweit **432,5 Millionen öffentliche Wi-Fi-Hotspots gibt**. Und im Jahr 2022 wurde festgestellt, dass 16 % der Nutzer*innen sensible Daten preisgeben, indem sie sich mit riskanten Hotspots verbinden. Wenn man davon ausgeht, dass sich nur ein Nutzer*innen mit jedem riskanten Hotspot verbindet, wären das 432,5 Millionen Nutzer*innen, die Daten über nicht vertrauenswürdige Netzwerkverbindungen übertragen.

Die Zahlen unterscheiden nicht zwischen Unternehmens- und Privatanwendern und berücksichtigen auch keine Endgeräte-Sicherheitslösungen, die bei der Vereitelung von Phishing-Angriffen helfen können, wie z. B. Content-Filter-Software, die explizit den Zugriff auf bösartige URLs und Domains im Zusammenhang mit Phishing-Kampagnen verhindert.

Vor allem aber berücksichtigen sie laut EC-Council nicht **wie Sie Ihre Mitarbeiter*innen am besten schützen** können. Ganz gleich, ob es um die Bekämpfung von Social-Engineering-Bedrohungen oder die Abwehr von Phishing-Angriffen über eine beliebige Anzahl von Kommunikationsmedien geht, eine der besten Abwehrmaßnahmen ist keine Sicherheitskontrolle, sondern eine Verwaltungsmaßnahme - die **Schulung des Bewusstseins für Cybersicherheit**. Mit einem umfassenden Benutzerschulungsprogramm, das in Ihre Onboarding-Prozesse integriert ist, und regelmäßigen Aktualisierungen, die genau auf die Angriffe abgestimmt sind, denen unzählige Unternehmen weltweit zum Opfer fallen, erhalten die Benutzer*innen das nötige Wissen, um Bedrohungen zu erkennen und die Risiken einzuschätzen, die mit der Durchführung von Phishing-Versuchen verbunden sind.

Die Investition in Schulungsprogramme für das Sicherheitsbewusstsein der Unternehmensakteur*innen ist ein wichtiger Bestandteil der Sicherheitsstrategie eines Unternehmens und sollte nicht übersehen werden. Dies bedeutet, dass für die Endbenutzer*innen fortlaufende, vielseitige Schulungen durchgeführt werden müssen, die eine Vielzahl von Best Practices abdecken und die Benutzer*innen über die neuesten Bedrohungen aufklären, von denen sie am ehesten betroffen sind. Dies wird sie in die Lage versetzen, neue und sich entwickelnde Angriffe zu erkennen und proaktive Maßnahmen zur Verbesserung ihrer Sicherheitshygiene zu ergreifen — sowohl bei der Arbeit als auch im Privatleben.

Die 10 wichtigsten Arten von Phishing-Angriffen sind:

1. **E-Mail:**
   E-Mail-Nachrichten werden an Personen gesendet, die vorgeben, von einer seriösen, vertrauenswürdigen Quelle zu stammen.

2. **Vishing:**
   Voice-Phishing-Angriffe wechseln das Medium zu einem telefonorientierten Angriff (TOAD), wobei häufig die Nummer des Anrufers/der Anruferin gefälscht wird, um sich als vertrauenswürdige Quelle auszugeben. Wie die betrügerischen Anrufe, die behaupten, vom FBI zu sein.

3. **Smishing:**
   Ähnlich wie beim Vishing verwenden Bedrohungsakteure SMS-Nachrichten mit Links oder Anhängen anstelle von Anrufen, um Benutzer*innen von Mobilgeräten zu kompromittieren.

4. **Social Media/Angler:**
   Neue Technologien bringen neue Angriffsvektoren hervor, weshalb diese Angriffe auf Nutzer*innen sozialer Medien über verschiedene Plattformen hinweg abzielen. Bei letzterem, dem Angler-Phishing, handelt es sich um eine neuere Variante des Social-Media-Themas, bei der sich Angreifer als Kundendienstmitarbeiter*innen ausgeben, oft mit einem gefälschten Profilkonto, um Opfer anzusprechen, die Hilfe benötigen.

5. **Spear:**
   Eine Variante des E-Mail-Phishings, die stattdessen einen gezielten Ansatz verfolgt und sich auf bestimmte Personen innerhalb eines Unternehmens konzentriert, z. B. auf einen Mitarbeiter/eine Mitarbeiterin der Lohnbuchhaltung.

6. **Whaling:**
   Ähnlich wie Spear-Phishing zielt dieser Angriff auf Führungskräfte und C-Suite-Mitglieder*innen ab.

7. **HTTP/S:**
   Website-basierte Angriffe, die URLs verwenden, die oft subtile Rechtschreibfehler enthalten, die auf den ersten Blick schwer zu erkennen sind, wie z. B. „iamf.com” statt jamf.com. Dazu können auch SSL-gesicherte Domänen gehören, die rechtmäßig registriert sind, um die Sicherheitsprüfungen in modernen Browsern zu umgehen.

8. **Website-Fälschung:**
   Diese Angriffsart geht häufig mit HTTP/S-Angriffen einher. Dabei wird neben der bösartigen URL eine legitim aussehende Website mit dem Originaltext, den Logos, Farbschemata und Funktionen erstellt, die die tatsächliche Website widerspiegelt und ein vertrauenswürdiges Erscheinungsbild und Gefühl vermittelt.

9. **Watering Hole:**
   Watering Hole-Angriffe sind teils Spear-Phishing, teils taktische Angriffe, die auf bestimmte Benutzergruppen und eine von ihnen häufig besuchte Website abzielen. Der Angriff zielt darauf ab, die Website zu kompromittieren und sie mit Malware zu infizieren, sodass die betroffenen Benutzer*innen beim Besuch der Website ebenfalls infiziert werden.

10. **Pop-up:**
    Wie die Pop-up-Werbung früherer Zeiten erfordert diese Phishing-Variante, dass böswillige Akteur*innen eine Website mit Malware infizieren, dann eingebettete Werbung oder neuere, von den Benutzer*innen aktivierte Benachrichtigungen nutzen und die Benutzer*innen infizieren, wenn die Nutzlast geliefert wird.

Trend 2 - Die Privatsphäre der Benutzer*innen hat einen Platz am Sicherheitstisch

Hersteller und Entwickler*innen wie Apple und Jamf rühren seit einiger Zeit kräftig die Datenschutztrommel. Im Allgemeinen haben andere Technologieanbieter*innen in der Vergangenheit dem Schutz der Privatsphäre nicht den gleichen Stellenwert eingeräumt wie anderen Sicherheitsmaßnahmen in ihren Hardware- und Softwareangeboten.

Ebenso wie die Folgen des Bekanntwerdens von persönlichen und geschäftlichen Daten bringt auch der Kampf um den Schutz von Nutzerdaten viele Opfer mit sich, wenn sie verletzt werden. Bedenken Sie, dass personenbezogene Daten nicht einfach ohne die Zustimmung des Nutzers/der Nutzerin gesammelt werden. Sie ist in mehrfacher Hinsicht gefährdet:

- Nationalstaaten verwenden bösartigen Code, der das Abhören von Kommunikationsdaten ermöglicht, wie z. B. das Mikrofon der Kamera oder die Aufzeichnung der Tasten auf den Geräten der Opfer, um diese auszuspionieren.
- Böswillige Akteur*innen nutzen diese Daten zur persönlichen oder finanziellen Bereicherung sowie zur Ausweitung von Social-Engineering-Kampagnen und zur Erpressung der Opfer.
- Unternehmen bereichern sich, indem sie gesammelte Daten ohne Zustimmung der Nutzer*innen an Werbetreibende und/oder Drittpartner*innen verkaufen.

In anderen Fällen geraten Unternehmen, die personenbezogene Daten im Rahmen ihrer legitimen Betriebsabläufe erfassen, in Schwierigkeiten, weil sie nicht ausreichend geschützt sind, um personenbezogene Daten vor externen Angriffen, Bedrohungen durch Insider oder gesetzlichen Vorschriften zu schützen. Und in einigen Fällen **sind sich Unternehmen der Bedrohung nicht einmal bewusst,** wie die Tatsache zeigt, dass „5 % der Unternehmen im Jahr 2022 eine potenziell unerwünschte Anwendung in ihrer Geräteflotte installiert haben."

Auf den ersten Blick scheinen 5 % nicht signifikant zu sein. Doch die Risikobewertung geht weit über bloße Zahlen hinaus. Dabei werden folgende Punkte berücksichtigt:

- Identifizierung von Zielwerten
- Alle vorhandenen Angriffsvektoren
- Arten von möglichen Angriffen
- Wahrscheinlichkeit des Auftretens eines Angriffs
- Mögliche Auswirkungen, wenn sie ausgenutzt oder kompromittiert werden

Diese Kombination ermöglicht es den Unternehmen, die vorhandenen Risiken und ihre Auswirkungen auf die Geschäftskontinuität zu bewerten. Was bedeutet das für personenbezogene Daten?

„**0,4 %** der Android-Geräte hatten im Jahr **2022** eine potenziell unerwünschte App installiert, verglichen mit **0,1 %** der iOS Geräte."

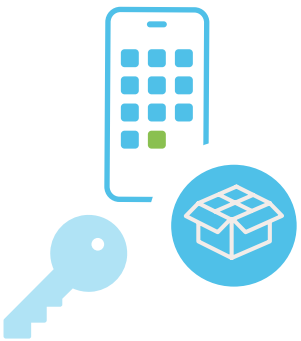
Android ist ein offenes Ökosystem, das zu mehr riskanten Apps führt. Apple hat ein kuratiertes App-Ökosystem geschaffen und bietet einen strengeren Schutz der Privatsphäre der Nutzer*innen, der die Einführung dieser riskanten Apps einschränkt.

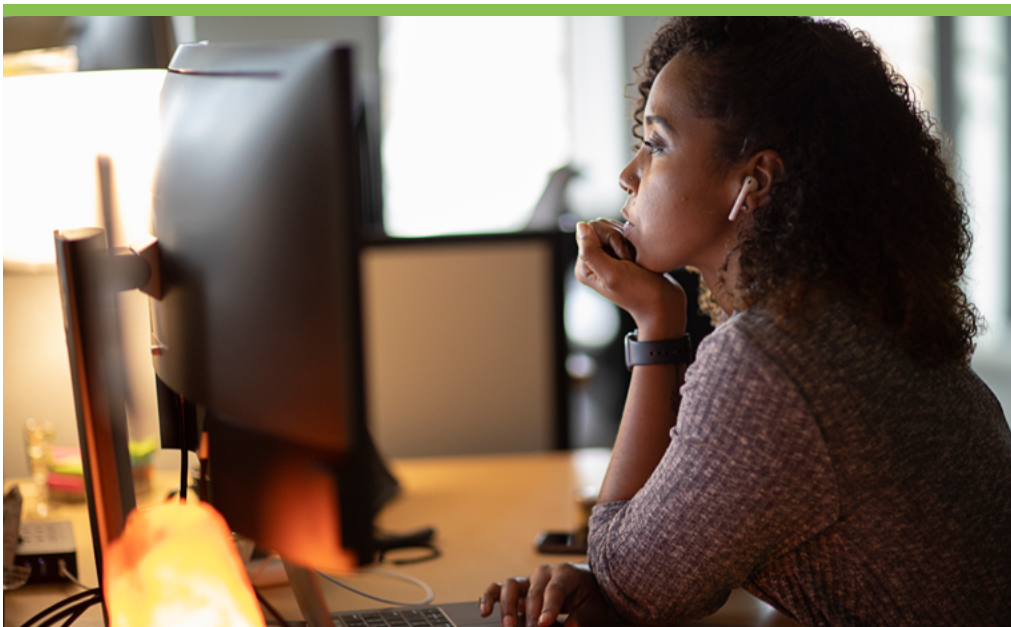
Der letzte Punkt in Bezug auf die potenziellen Auswirkungen eines Missbrauchs oder einer Kompromittierung darf nicht unterschätzt werden, da er direkt den Kern der regulatorischen Kontrollen und deren Arbeit zur Risikominderung trifft, indem er Datenlecks verhindert, die gegen gesetzliche Vorschriften verstoßen würden (mehr über die Einhaltung von Vorschriften später in diesem Bericht).

Wirksame Datenschutzkontrollen gewinnen neben den Sicherheitskontrollen immer mehr an Bedeutung — nicht nur, um bei Bedarf die Einhaltung von Vorschriften durchzusetzen, sondern auch, um die Preisgabe von Nutzerdaten als Teil einer umfassenden Sicherheitsstrategie zu begrenzen. Sie muss sich auf alle Lösungen, Prozesse, Beteiligten und Arbeitsabläufe innerhalb eines Unternehmens erstrecken, um die Datensicherheit insgesamt zu gewährleisten, und zwar parallel zur Entwicklung oder Implementierung aller Komponenten im gesamten Unternehmen — und nicht als nachträgliche Maßnahme.

Verwaltungslösungen helfen dabei, die Unternehmensrichtlinien mit den gesetzlichen Anforderungen in Einklang zu bringen und den Verwaltungsaufwand zu verringern, indem die IT-Abteilung die Unternehmensapps benennen kann. Dadurch wird sichergestellt, dass alle Datentypen in der gesamten Infrastruktur unabhängig von Gerätetyp und Standort gesichert sind.

Durch die Verwaltung mehrerer Geräteeigentumsmodelle schaffen Unternehmen ein Gleichgewicht zwischen der Sicherung von Apps und Daten und der Anwendung sicherer Konfigurationen auf die Geräte selbst, um sicher auf Unternehmensressourcen zuzugreifen, während die Benutzer*innen letztlich die Kontrolle über die privaten Daten haben, die mit ihren persönlichen App und der Gerätenutzung verbunden sind. Unternehmen schützen firmeneigene Daten, die sowohl sensibel als auch vertraulich sind, während sie gleichzeitig einen „Hands-Off"-Ansatz für private Nutzerdaten **beibehalten, der es den Endnutzer*innen ermöglicht, den Grad des Zugriffs** auf diese Daten zu kontrollieren, wodurch der Datenschutz insgesamt weiter verbessert wird, unabhängig davon, ob die Geräte Teil eines BYOD-Programms, unternehmenseigene Geräte, die Teil einer CYOD/COPE-Initiative sind, oder eine Mischung dieser Modelle sind.





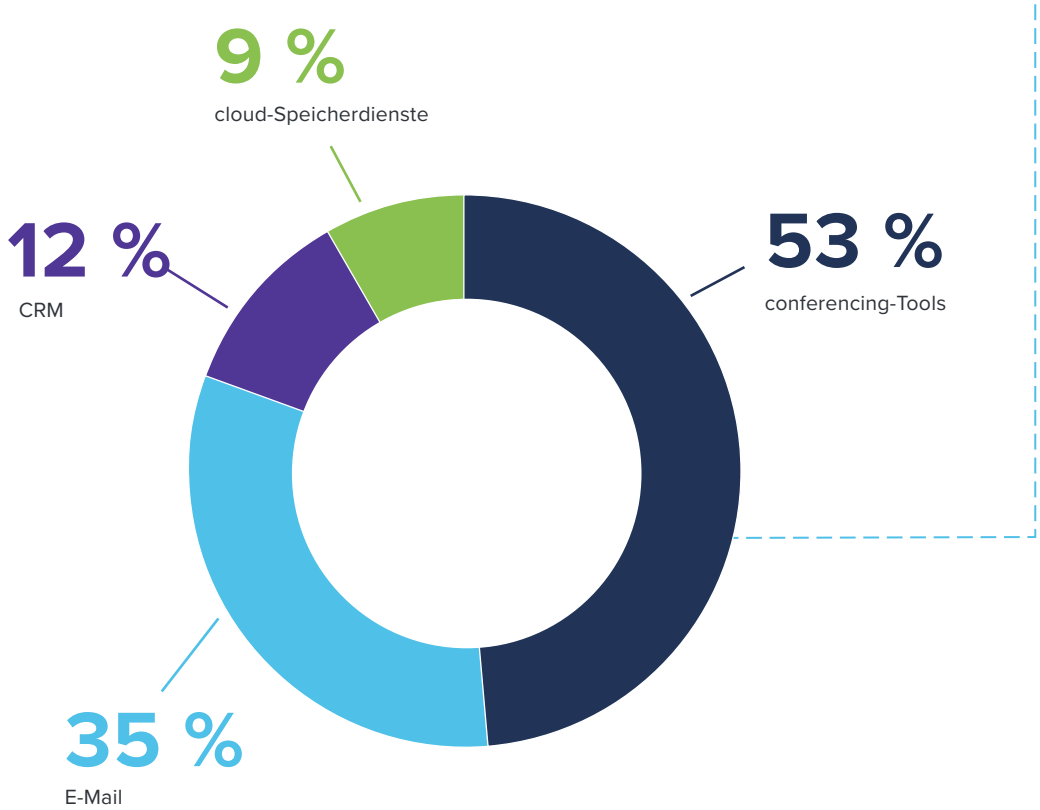
Trend 3 – Böse Akteur*innen konvergieren Angriffe zu neuen Bedrohungen

Eine gute Nachricht an der macOS Malware-Front: Die Gesamtzahl der Malware-Infektionen zeigte keine Anzeichen für ein Wachstum im Vergleich zum Vorjahr. Die gute Nachricht: Im Jahr 2022 sank die Zahl der **neuen Malware-Infektionen** von knapp über 150 Millionen auf etwa 100 Millionen, wie aus der laufenden Registrierung von Schadprogrammen und potenziell unerwünschten Apps (PUA) durch AV-Atlas hervorgeht.

Bösartiger Netzwerkverkehr, der sich auf netzwerkbasierte Indikatoren für eine Gefährdung (Indicators of Compromise, IoCs) bezieht, die in den Kommunikationsmustern zwischen dem Gerät und den Internetservern beobachtet werden können, tritt immer häufiger auf. 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 aktive Überwachung der Gesundheit der Endpunkte bei der Bewertung kombinierter Risikofaktoren so wichtig.

Bösewichte, die verschiedene Angriffe miteinander kombinieren, sind an sich nichts Neues. In der modernen Bedrohungslandschaft werden jedoch immer mehr dieser konvergierten Bedrohungen aktiv eingesetzt, um verteilte Mitarbeiter*innen auf neue Art und Weise anzugreifen und sich unbefugten Zugriff auf geschützte Dienste und Ressourcen zu verschaffen. In einem einzigen Monat des Jahres 2022 griffen 53 % der kompromittierten Geräte auf Conferencing-Tools zu, während 35 % auf E-Mails, 12 % auf ein CRM und 9 % auf Cloud-Speicherdienste zugriffen.

In einem einzigen Monat des Jahres 2022 griffen **53 %** der kompromittierten Geräte auf Conferencing-Tools zu, während **35 % auf E-Mails, 12 % auf ein CRM** und **9 % auf Cloud-Speicherdienste zugriffen.**



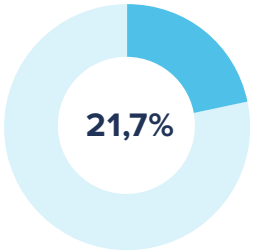
Beispiel für einen raffinierten Angriff

Ein Mitarbeiter/eine Mitarbeiterin erhält eine Spear-Phishing-Nachricht, die scheinbar von einem Kollegen/einer Kollegin stammt. Die Nachricht enthält einen Link zu einem „Arbeitsdokument", das bösartigen Code auf dem Gerät des Opfers einschleust, der dessen Anmeldeinformationen sammelt und gleichzeitig eine Ransomware-Nutzlast übermittelt. Während er die sensiblen Daten erbeutet, nutzt der Angreifer/die Angreiferin die Anmeldeinformationen, um weiteren Zugriff auf die Infrastruktur des Unternehmens zu erhalten. Schließlich erfüllt der Schädling noch zwei weitere Funktionen: Er fügt den Endpunkt in ein Botnet ein, das für Angriffe auf andere Organisationen genutzt wird, und sucht nach weiteren Geräten, die er infizieren kann, um den Prozess zu erweitern und das Botnet zu vergrößern.

Die übergreifende Botschaft ist, dass Angriffe mehr als nur eine Form annehmen können, dass sie über einen beliebigen Zeitraum erfolgen können und dass sie oft unentdeckt bleiben. Einige Angriffsketten treten kurz nach der Kompromittierung auf, wie z. B. Ransomware, während andere eher taktischer Natur sind und mehr Zeit benötigen, wie z. B. der Aufbau eines Botnetzes, um Systeme mit DDoS-Angriffen (Denial of Distributed Service) anzugreifen.

Diese Konvergenz ist schwer zu bekämpfen, da die Opfer in der Regel das Ausmaß des Angriffs erst erkennen, wenn die nächste Welle auf sie zukommt. Bestimmte Praktiken können jedoch einige Risiken mindern und die Auswirkungen anderer Risiken stark einschränken oder abmildern. Die aktive Überwachung von Endgeräten und das Sammeln von Telemetriedaten über den Gesundheitszustand von Endgeräten ist für Administratoren von entscheidender Bedeutung, da sie einen tiefen Einblick in die Geräte und deren Zustand in Bezug auf verschiedene Vektoren, wie z. B. Patch-Levels, bietet, insbesondere da verdächtige Verhaltensweisen, die auf eine Gefährdung des Geräts hinweisen können, vom Endbenutzer/von der Endbenutzerin nicht gesehen oder wahrgenommen werden.

Apropos Patch-Verwaltung: Die Verwaltung des Lebenszyklus von Apps ist eine Grundvoraussetzung, um das Risiko von Systemschwachstellen zu mindern und gleichzeitig sicherzustellen, dass die Apps über ein Höchstmaß an Sicherheit zum Schutz vor bekannten Bedrohungen verfügen. Dies ist besonders wichtig, wenn man bedenkt, dass App-Stores von Drittanbieter*innen oft Versionen legitimer Apps anbieten, die bösartigen Code enthalten und die Geräte der Benutzer*innen infizieren. Stellen Sie sich vor, die kostenlosen Versionen von kostenpflichtigen Apps dienen als Köder, um Opfer anzulocken.



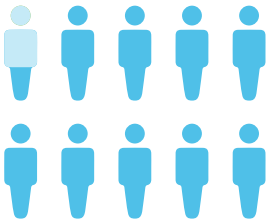
21,7 % der Android Geräte griffen auf App-Stores von Drittanbieter*innen zu, verglichen mit **0,002 %** der **iOS Geräte.**

App-Stores von Drittanbieter*innen sind ein gängiger Weg, um den App-Prüfprozess zu unterlaufen, der Geräte und Nutzer*innen schützt.

0,02 % der Android Geräte wurden verwurzelt und **0,001 %** der **iOS Geräte** wurden im Jahr 2022 **geknackt**

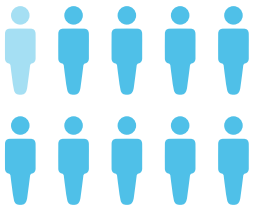
Trotz des geringen Prozentsatzes ist es bemerkenswert, dass die Anzahl der betroffenen Android-Geräte doppelt so hoch ist wie die von Apple. Und wenn man sich die abstrakte Menge an Android und Apple Geräten in der Welt vor Augen führt, kann man sich das Ausmaß dieser Entwicklung gut vorstellen.

Während bestimmte Betriebssysteme das Side-Loading von Anwendungen zulassen, müssen andere, wie z. B. iOS, erst geknackt werden, um den Schutz zu umgehen, der iOS basierte Geräte vor der Ausführung von unsigniertem Code schützt. Das Sperren von Geräten ist nur ein Teil der Gleichung. Es ist von entscheidender Bedeutung, geknackte Geräte in Echtzeit zu identifizieren, um diesen Bedrohungsvektor wirksam zu beseitigen.



0,004 % der Nutzer und **0,3 %** der Unternehmen hatten im Jahr 2022 ein **geknacktes** oder **verwurzeltes** Gerät.

Die Statistik des letzten Jahres:



Weniger als 1 % der Unternehmen hatten 2021 ein **geknacktes** oder **verwurzeltes** Gerät.

Angriffe in der Lieferkette

Angriffe auf die Lieferkette oder auf **Dritte** haben in der Vergangenheit breitere Auswirkungen gehabt, die mehrere Schichten tief in und durch Organisationen in der Pipeline gehen, bevor sie **das eigentliche Ziel des Angreifers/der Angreiferin erreichen.** Die Auswirkungen sind oft weitreichend und betreffen Unternehmen auf der ganzen Welt, unabhängig davon, wie gut ihre Sicherheitsvorkehrungen sind.

Die Verhinderung dieser Angriffe ist ein schwieriges Unterfangen, vor allem weil die Unternehmen nicht die Befugnis haben, von jedem Unternehmen (oder dessen Auftragnehmern) in der Pipeline zu verlangen, die Risikofaktoren sinnvoll zu mindern. Leider gilt dies aus denselben Gründen auch für den Schutz Ihres Unternehmens vor diesen Bedrohungen. Doch wie die Cybersecurity and Infrastructure Security Agency (CISA) und das National Institute of Standards and Technology (NIST) in ihrem gemeinsamen technischen Dokument **Defending Against Software Supply Chain Attacks (Verteidigung gegen Angriffe auf die Software-Lieferkette**) betonen, besteht ein Schlüsselelement zur Stärkung der Fähigkeit einer Organisation, solche Angriffe zu verhindern, abzuschwächen und darauf zu reagieren, in der Einhaltung branchenüblicher Best Practices als Teil einer umfassenden Defense-in-Depth-Sicherheitsstrategie, zu der auch die Überprüfung der Sicherheitsprozesse von Zulieferern durch unabhängige Prüfer*innen gehört, um sicherzustellen, dass Ihre Partner*innen (und in der Folge auch deren Partner*innen) die richtigen Abhilfemaßnahmen ergreifen, bevor ein Angriff erfolgt.

Trend 4 – Die Einhaltung von Vorschriften ist Teil des Sicherheitssystems

Ein zunehmender Trend ist neben der Sicherheit von Unternehmensdaten auch die Bedeutung des Datenschutzes für die Nutzer*innen. Dies gilt vor allem für die Einhaltung von Vorschriften, insbesondere von Landes-, Bundes- und Regionalvorschriften. Denken Sie nur daran, wie die Allgemeine Datenschutzverordnung (GDPR) und das kalifornische Verbraucherschutzgesetz (CCPA) den Schutz der Rechte der Nutzer*innen auf Privatsphäre auf nationaler bzw. bundesstaatlicher Ebene verbessern, oder wie Fintech – eine der am stärksten regulierten Branchen weltweit – mehreren Facetten der Governance unterliegt.

Im Folgenden finden Sie einige Beispiele dafür, wie mehrere Rechtsvorschriften entweder allein oder in Verbindung mit anderen zur Einhaltung von Vorschriften in bestimmten Branchen beitragen:

Sarbanes-Oxley Act von 2002 (SOX): schreibt bestimmte Bedingungen für die Rechnungslegungspraxis vor

Gramm-Leach-Bliley-Gesetz (GLB): Festlegung eines Mindestmaßes an Cybersicherheitsschutz, das zur Aufrechterhaltung der Informationssicherheit erforderlich ist

Financial Industry Regulatory Authority (FINRA): beschreibt ausdrücklich, wie sich die Geschäftsprozesse auf die Gewährleistung des Anlegerschutzes durch faire und ehrliche Geschäfte in der Wertpapierbranche beziehen

In Anbetracht der Compliance-Vorschriften, die sich auf Unternehmen in bestimmten Branchen auswirken, und ihrer globalen Reichweite, die von den betroffenen Unternehmen die Einhaltung von Gesetzen verlangen, die sich möglicherweise weit außerhalb ihres Zuständigkeitsbereichs befinden, müssen Unternehmen eine stärkere Kontrolle über Arbeitsabläufe ausüben, um den Datenschutz und die Verwaltung geschützter Datentypen - wie personenbezogene Daten (PII), geschützte Gesundheitsdaten (PHI) und Business Intelligence-Daten (BII) - zu gewährleisten, wenn diese nach den Wünschen der Benutzer*innen und/oder gemäß den Vorschriften erfasst, verarbeitet, gespeichert, geändert, freigegeben und vernichtet werden.

Die Einhaltung der Vorschriften kann eine schwierige Aufgabe sein, die ernsthafte Überlegungen, Verwaltung und Unterstützung erfordert, selbst wenn Ihre Geräte und Daten von der Organisation verwaltet werden. Aber wie sieht es mit der Durchsetzung der Vorschriften bei einer verteilten Belegschaft aus, die in der Lage sein muss, von überall, auf jedem Gerät und zu jeder Zeit auf Unternehmensressourcen zuzugreifen? Die zusätzlichen Komplikationen, die sich aus der Kombination von On-Premise- und Remote-/Hybrid-Arbeitskräften ergeben, können für Unternehmen, die Compliance-Anforderungen erfüllen und sich in der modernen Bedrohungslandschaft zurechtfinden müssen, zu einem Problem werden.

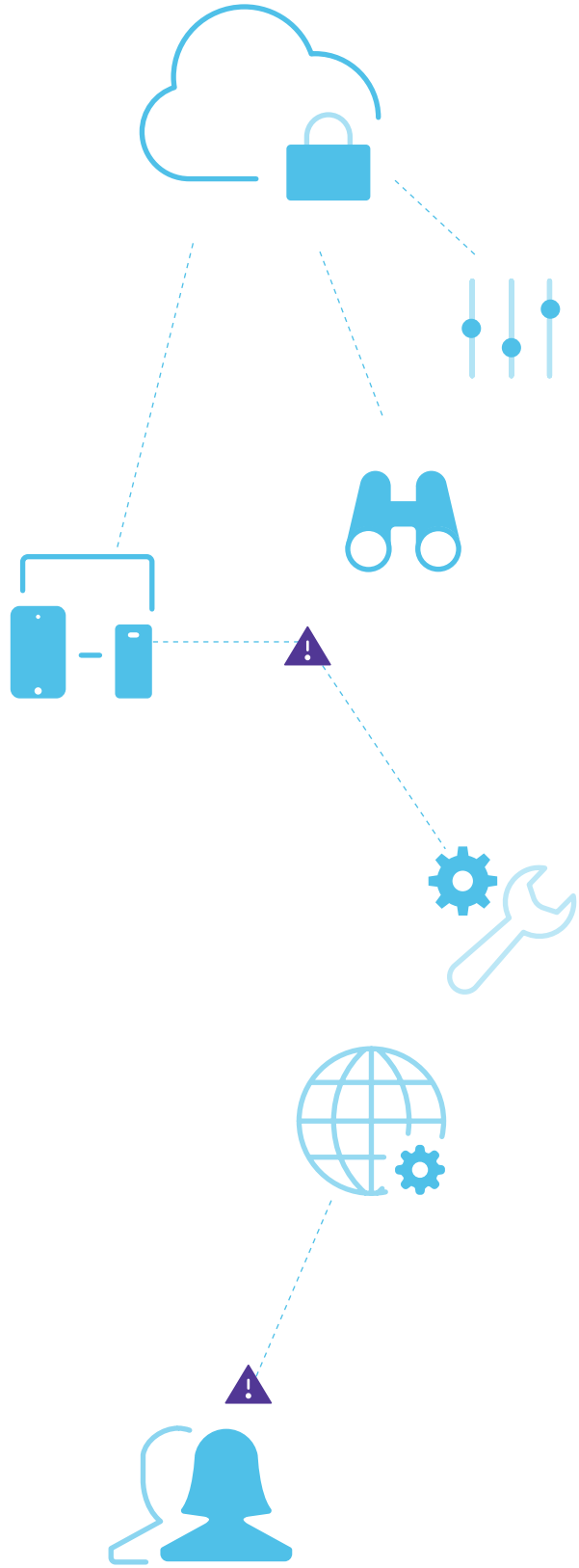
„Im Jahr **2022 nutzten 21 %** der Mitarbeiter*innen Geräte, die falsch **konfiguriert waren,** was sie einem **Risiko aussetzte."**

Leider wird die Einhaltung der Vorschriften nur noch schwieriger, wenn auch noch Geräte in persönlichem Besitz dazukommen. Im Jahr 2022 nutzten 21 % der Mitarbeiter*innen Geräte, die falsch konfiguriert waren, und setzten sich damit einem Risiko aus. Mehr noch, es besteht die Gefahr, dass sensible, vertrauliche oder unternehmenskritische – und möglicherweise regulierte – Daten offengelegt werden, was wiederum das Unternehmen (und möglicherweise auch den Nutzer*innen) zivil- und/oder strafrechtlich haftbar macht, wenn Verstöße gegen gesetzliche Vorschriften festgestellt werden.

Zwar haben viele Unternehmen eine Form von BYOD- oder Mitarbeiterwahlprogrammen eingeführt, die es den Endbenutzer*innen ermöglichen, die Gerätetypen und Betriebssysteme auszuwählen, mit denen sie am produktivsten sind und sich am wohlsten fühlen, doch die Lösung für ein effektives Compliance-Management kann nicht nur darin bestehen, alle Geräte mit Ausnahme der verwalteten Geräte auszusperren. **Wir haben festgestellt, dass 8 % der Benutzer*innen und 21 % der Unternehmen von Konfigurationsschwachstellen betroffen sind**, was bedeutet, dass sogar unternehmenseigene und verwaltete Geräte betroffen sein können. Lösungen müssen mehr berücksichtigen, um über die Geräteverwaltung hinaus auf Sicherheitsfragen zu reagieren.

Tatsache ist, dass jeder Endpunkt zu jeder Zeit einen Patch verpassen, Daten aufgrund einer Sicherheitslücke verlieren oder einfach verloren gehen oder gestohlen werden kann. In jedem Szenario wäre eine andere Maßnahme zur Risikominderung erforderlich. Einige Situationen können über automatisierte Reaktions- und Abhilfeworkflows gehandhabt werden, aber es wird immer auch einen Platz für manuelle Abhilfemaßnahmen geben.

Wie bei den meisten sicherheitsrelevanten Diskussionen gibt es keine Patentrezepte oder Einheitslösungen, die alles abdecken, was notwendig ist, um Ihre Infrastruktur jederzeit konform zu halten. Wir empfehlen die Implementierung einer umfassenden Sicherheitsstrategie, die mehrere konvergierende Lösungen bietet, um Ihre individuellen Compliance-Anforderungen aus vielen Blickwinkeln zu erfüllen.



Trend 5 – Die Sicherung von Daten in entfernten/hybriden Umgebungen ist immer noch eine Herausforderung

Die Umstellung auf eine dezentrale Belegschaft hat einen Wandel bei der Sicherung von Benutzer*innen, Daten und Geräten eingeleitet. Mit der effektiven Aushöhlung des Netzwerkrands wurden lokale Lösungen durch Cloud-basierte Lösungen ersetzt, um Sicherheitsdienste an Benutzer*innen zu verteilen, die mit jedem Gerät von überall aus arbeiten. Das Ergebnis war eine Endgeräte-Sicherheitslösung, die leistungsfähiger und unabhängiger ist und über zusätzliche Ausfallsicherheit und robuste Appsicherheit verfügt.

Doch trotz der festgestellten Vorteile sehen sich Unternehmen auch noch mehrere Jahre nach der Migration mit Problemen bei der Datensicherheit in entfernten und hybriden Arbeitsumgebungen konfrontiert. Leider gibt es keinen eindeutigen Hinweis auf den Schuldigen. Ein Bündel von Problemen trägt zu einer unzureichenden Datensicherung bei. Einige dieser Probleme sind auf einen Mangel an Wissen zurückzuführen:

- Echtzeit-Einblick in den Zustand der Endgeräte
- Integration von Verwaltungs- und Sicherheitswerkzeugen
- Automatisierte Prozesse und Arbeitsabläufe
- Dezentralisierte Protokollierung und Bedrohungsdaten
- Durchsetzung von Richtlinien und Vorschriften
- Sicherheitstrainingsprogramme für Endbenutzer*innen
- Best-of-breed-Lösungen
- Risikobewertungspraktiken zur Ermittlung von Vermögenswerten und Bedrohungen

So haben wir beispielsweise festgestellt, dass **64 % der anfälligen Geräte auf Tools für die Zusammenarbeit und 34 % auf Unternehmens-E-Mails zugreifen.** Dies deutet darauf hin, dass, obwohl Risiko- und Kompromissindikatoren subjektiv sind und von Unternehmen zu Unternehmen variieren, Routineaufgaben wie die Patch-Verwaltung nicht auf allen Geräten durchgeführt werden. Dadurch sind nicht nur die Geräte selbst, sondern auch die Unternehmensressourcen gefährdet. Es geht sogar über Apps und Konfigurationen hinaus. Jamf Threat Labs fand heraus, dass **1 von 5 Geräten ein nicht aktuelles Betriebssystem verwendet.** Für den Schutz von Benutzer*innen und Unternehmen ist es wichtig, dass die Sicherheit auf allen Ebenen einer Defense-in-Depth-Strategie gegeben ist, angefangen bei der Betriebssystemebene.

Dies verdeutlicht, wie wichtig es ist, einen Überblick über Ihre Geräteflotte und deren Interaktion mit der Infrastruktur Ihres Unternehmens zu haben, insbesondere wenn Ihre Branche reguliert ist. Diese Anforderung wird noch verstärkt, wenn man bedenkt, dass die meisten Aufsichtsbehörden verlangen, dass Unternehmen die Einhaltung der Vorschriften durch regelmäßige Audits nachweisen, die von den Aufsichtsbehörden durchgeführt werden, um zu überprüfen, ob geschützte Daten und die Endpunkte, die mit ihnen interagieren, in Übereinstimmung mit den gesetzlichen Vorschriften gesichert sind.

Die Bewertung der Anlagen und Bedrohungen, die Ihr Unternehmen betreffen, und die begleitende Telemetrie zur Identifizierung der betroffenen Endgeräte sind jedoch nur ein Teil der Lösung. Es werden moderne Lösungen benötigt, um Risiken zu mindern und Zugangsentscheidungen in Echtzeit durchzusetzen. Veraltete Technologien wie VPN zur Sicherung von Remote-Verbindungen können sicherlich nicht mit neueren Technologien konkurrieren, die für die Herausforderungen verteilter Arbeitsplätze und der modernen Bedrohungslandschaft entwickelt wurden. ZTNA erlaubt Verbindungen zu App und Diensten erst dann, wenn überprüft wurde, ob das Gerät und der Benutzer auf die angeforderten Dienste zugreifen dürfen und die Mindestanforderungen für einen sicheren Betrieb erfüllen.

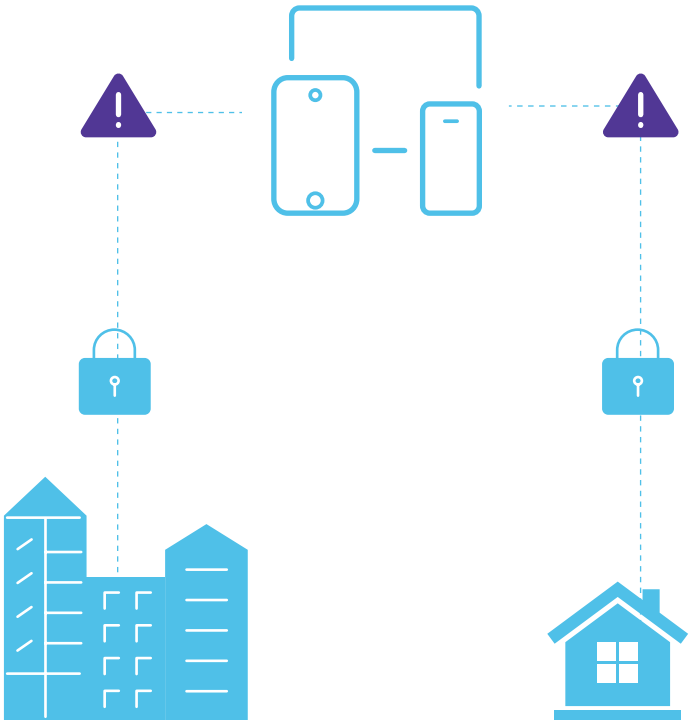
Die Lösungen von ZTNA wurden für moderne Netzwerke und Arbeitsabläufe entwickelt, um Risiken zu minimieren und Daten zu schützen. Gleichzeitig sind sie flexibel genug, um sicherzustellen, dass persönliche Apps und Daten privat bleiben. Darüber hinaus können sich autorisierte Benutzer*innen nur mit den Apps verbinden, auf die sie zugreifen dürfen, und zwar nach dem Prinzip der geringsten Privilegien, während der Geschäftsverkehr durch Mikrotunnel geleitet wird. Dies verhindert, dass Angreifer*innen, die einen einzelnen Benutzer*innen kompromittieren, auf alle Apps zugreifen können, für die der Benutzer eine Zugriffsberechtigung hat. Durch die integrierte Segmentierung von Verkehrstunneln werden Angreifer*innen daran gehindert, sich seitlich im Netzwerk zu bewegen, wodurch Bedrohungen effektiv eingeschränkt werden.

Ein weiterer wichtiger Punkt ist die sichere Integration von Lösungen durch die Nutzung von APIs, um kritische Telemetrie- und Endgerätezustandsdaten mit Lösungen auszutauschen, die die Erfolgsrate von Bedrohungen für Geräte, Benutzer*innen und sensible Daten begrenzen. Dies steht in krassem Gegensatz zu „Bolt-on"- oder Standalone-Lösungen, bei denen Sicherheits-Tools von der Stange unabhängig voneinander arbeiten, denen aber die Integrationskomponente fehlt, die eine ganzheitliche Defense-in-Depth-Lösung ausmacht.

In dem Maße, in dem bösartige Akteur*innen ihre Tools weiterentwickeln, müssen Unternehmen ihre Lösungen so einsetzen, dass sie bekannte Angriffe verhindern und gleichzeitig das Risiko neuer Angriffe mindern. Aus diesem Grund wächst und gedeiht die Bedrohungsjagd in Unternehmen, die ihre IT- und Sicherheitsteams dabei unterstützt, unbekannte und neuartige Bedrohungen zu identifizieren, abzuschwächen und zu beseitigen, bevor sie zu Datenverletzungen führen können. Künstliche Intelligenz (KI) und maschinelles Lernen (ML) haben ihre Effektivität in verschiedenen Branchen bewiesen, und die Cybersicherheit ist eine davon, da Lösungen zunehmend die erweiterte Verarbeitungsleistung und die Verhaltensanalysefähigkeiten nutzen, um Bedrohungsakteure und ihre Angriffe mit einer Geschwindigkeit zu erlernen, effizient vorherzusagen und abzuwehren, mit der menschliche Administrator*innen einfach nicht mithalten können.

Zentrieren Sie Ihre Strategie auf die Verwaltung mobiler Geräte (MDM), um sowohl persönliche als auch unternehmenseigene Geräte zu schützen und Patches auf dem neuesten Stand zu halten. Setzen Sie Endpunktsicherheit ein, um Malware zu verhindern, und sammeln Sie gleichzeitig umfangreiche Telemetriedaten durch aktive Überwachung der Endgeräte. Eine API ist eine großartige Möglichkeit, Bedrohungsdaten sicher zwischen diesen beiden Lösungen auszutauschen, und ermöglicht es Unternehmen, Compliance-Anforderungen durch richtlinienbasierte Durchsetzung einzuhalten. Die Hinzufügung von Identitäts- und Zugriffsmanagementlösungen zentralisiert die Verwaltung von Anmeldeinformationen und die Bereitstellung von Berechtigungen für genehmigte Unternehmensressourcen, während der Zugriff durch Multi-Faktor-Authentifizierung (MFA) gesichert wird.

Dies lässt sich in moderne Sicherheitslösungen wie ZTNA integrieren, um Verbindungen über jedes beliebige Netzwerk zu sichern, ML einzubinden, um neue Bedrohungen aufzuspüren, Angriffe zu stoppen, bevor sie beginnen können, und ältere VPNs durch moderne Lösungen zu ersetzen, die Zugriffsanfragen segmentieren, um netzwerkbasierte Bedrohungen abzuschwächen. Und schließlich erfassen Sie alle relevanten Bedrohungen und den Gerätestatus in Echtzeit, um das Management des Gerätelebenszyklus ganzheitlich zu automatisieren.



Empfehlungen

Da wir uns der Dreijahresmarke nähern, seit die weltweite Pandemie zu einem drastischen Wandel in globalen Arbeitsumgebungen geführt hat, hat sich der Schwerpunkt für viele von **„Wie setzen wir den Geschäftsbetrieb fort?"** zu **„Wie schützen wir Remote-Benutzer*innen und Unternehmensressourcen kontinuierlich verschoben."**

Einer der Hauptgründe für das Umdenken ist die Tatsache, dass IT- und Sicherheitsteams heute mehr als doppelt so viele Remote-Benutzer*innen unterstützen (46 %) wie vor der Pandemie (21 %), so der **Bericht The State of Security 2022** von Splunk. Die globale Untersuchung von Splunk hat ergeben, dass wir nicht nur immer mehr Angriffe, sondern auch mehr tatsächliche Sicherheitsverletzungen sehen

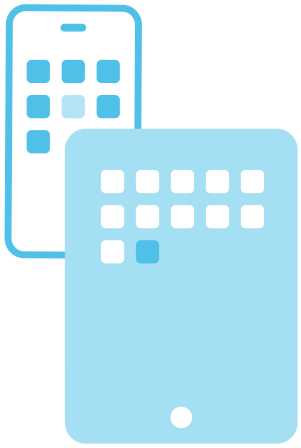
Diese Kombination aus steigenden Angriffszahlen, einer sich entwickelnden Bedrohungslandschaft und der wachsenden Notwendigkeit, Ressourcen zu sichern, auf die Remote-Benutzer*innen zugreifen, unterstreicht die Aussage des letztjährigen Security 360-Berichts:

> Sichere Fernzugriffslösungen müssen ausreichend flexibel und agil sein, um die Arbeit zu ermöglichen, ohne sie zu blockieren oder die Produktivität einzuschränken.

In diesem Jahr fügen wir dieser Aussage noch etwas hinzu:

> Endgerätesicherheit muss eine Konvergenz von Sicherheitslösungen bieten, die eine solide Grundlage und granulare Transparenz mit fortschrittlichen Technologien wie ML nutzen, um automatisierte sichere Workflows zu entwickeln, die mit Unternehmensrichtlinien und Branchenvorschriften übereinstimmen.

Letztlich sollten Unternehmen eine moderne, Cloud-basierte Defense-in-Depth-Sicherheitsstrategie entwickeln, die ihren individuellen Anforderungen von heute gerecht wird und gleichzeitig die Skalierbarkeit bietet, um die Anforderungen von morgen zu erfüllen.



Über diese Forschung

Wir wollen die wichtigsten Sicherheitstrends in der neuen Welt der hybriden Arbeit identifizieren. Die Informationen und Statistiken in diesem Papier sind die Ergebnisse unserer Analyse von Sicherheitstrends innerhalb einer Stichprobe von 500.000 durch Jamf geschützten Geräten, die iOS, macOS, iPadOS, Android und Windows in 90 Ländern über einen Zeitraum von 12 Monaten umfassen. Diese Analyse wurde im vierten Quartal des Jahres 2022 durchgeführt. Die in dieser Untersuchung analysierten Metadaten stammen aus zusammengefassten Protokollen, die keine persönlichen oder organisationsbezogenen Informationen enthalten. Mit dieser Analyse wollen wir keine Ängste schüren, sondern Sie und Ihre Benutzer*innen über die verfügbaren Optionen aufklären und darüber, wie Sie alle Aspekte der Geräte-, Benutzer*innen- und Unternehmensdaten am besten schützen können.