wandera
a Jamf company

Cloud Security Bericht 2021

Ein genauer Blick auf die Bedrohungen, denen die Daten Ihrer Organisation über Ihre wichtigsten Ressourcen, d. h. Ihre Endgeräte, Benutzer und Tools für den Fernzugriff, ausgesetzt sind, sowie praktische Hinweise, wie Sie Ihre geschäftlichen Tools konfigurieren können, um 2021 für alle Benutzer eine schnelle und sichere Konnektivität zu gewährleisten.

EMEA 45 Mortimer Street
London W1W 8HJ
+44 (0) 203 301 2660

USA 220 Sansome Street, Suite 1400
San Francisco CA 94104
+1 (415) 935 3095

Wichtige Ergebnisse

- In 52 % der Organisationen trat 2020 ein Malware-Angriff auf einem Remote-Gerät auf, was eine Steigerung von 41 % im Vergleich zu 2019 mit 37 % betroffenen Organisationen bedeutet.
- Von den 2020 durch Malware kompromittierten Mobilgeräten griffen 37 % nach der Kompromittierung weiterhin auf E-Mail-Nachrichten des Unternehmens zu und 11 % griffen weiter auf den Cloud-Speicher zu.
- In 28 % der Organisationen war 2020 regelmäßig ein Betriebssystem mit einer bekannten Sicherheitslücke im Einsatz.
- Verglichen mit der Zeit vor Beginn der Pandemie stieg die Anzahl der Aufrufe unangemessener Inhalte während der Arbeitszeit um bis zu 100 %.
- Auf Android-Geräten war die Wahrscheinlichkeit einer Installation gefährdender Apps um ein 5,3-faches höher als bei iOS-Geräten.
- Phishing-Angriffe traten zu Spitzenzeiten an Wochenenden um 6 % häufiger auf als zu Spitzenzeiten während der Arbeitstage.
- Im Jahr 2020 haben sich 4 % der Benutzer jede Woche mit einem riskanten Hotspot verbunden – im Vergleich zu 7 % im Jahr 2019, allerdings
- wiesen 15 % der Organisationen mindestens ein Gerät mit einer App auf, die Passwortdaten freigab, eine Steigerung gegenüber den 11 % im Vorjahr.

28 %

der Organisationen nutzten regelmäßig ein Betriebssystem mit einer bekannten Sicherheitslücke.

5,3 Mal höheres Risiko

Auf Android-Geräten war die Wahrscheinlichkeit eine gefährdete App zu installieren 5,3 Mal höher als bei iOS Geräten.

Einführung

Viele Organisationen mussten 2020 ihre Geschäftspraktiken komplett auf Mobilität umstellen und gleichzeitig das Produktivitätsniveau aufrechterhalten. Demzufolge wurde die IT-Rahmenvorgabe revidiert, um mehr Geräte, mehr Netzwerke und mehr Apps an mehr Orten als je zuvor zu unterstützen.

Die unternehmensinternen Grenzen sind gefallen. Eine Gartner-Befragung der leitenden Finanzdirektoren (CFOs) aus dem März 2020 zeigte, dass 74 % beabsichtigen, einige Mitarbeiter dauerhaft auf den mobilen Arbeitsplatz/das Homeoffice umzustellen.

Daraus folgt, dass wir beobachten können, wie die alten Maximen guter Sicherheitspraktiken sich vor unseren Augen verändern, um der neuen Normalität zu entsprechen. Die erfolgreichsten IT-Abteilungen konzentrieren sich darauf, ihren Benutzern alle Mittel bereitzustellen, damit sie fern vom Büro arbeiten können. Das erfordert einen flexibleren und agileren Umgang mit der Sicherheitsstrategie, um die unterschiedlichen Anforderungen der weit verbreitet arbeitenden Belegschaft zu erfüllen, und dazu bedarf es eines Modells, bei dem die Cloud an erster Stelle steht.

Bedeutende Branchenexperten sind der Ansicht, dass SASE (Secure Access Service Edge) das entscheidende Architekturmodell für innovative Unternehmen sein wird, die sich von der herkömmlichen Technologie weg bewegen, da SASE die Funktionen der Netzwerktechnik und Sicherheit in einem einheitlichen Cloud-nativen Dienst zusammenführt und abstimmt.

SASE mag das Zukunftsmodell sein, aber derweil müssen Unternehmen die richtigen Tools für die gegenwärtige Arbeit finden. Es ist wichtig, die Cyberrisiken zu verstehen und wie diese in Organisationen eindringen können, und genau das soll der Fokus dieses Jahresberichts sein.

Jedes Jahr analysieren wir die Bedrohungen, die die für die Arbeit genutzten Mobilgeräte betreffen. Mit laufender Entwicklung unseres Produktportfolios (inkl. Geräte, die über Smartphones und Tablets hinausgehen) hat sich auch unsere Perspektive auf eine mobile Belegschaft erweitert – sie arbeitet fern vom Büro und verwendet mehr als nur Mobilgeräte.

Der diesjährige Bericht befasst sich mit Bedrohungen und Sicherheitstrends, die echte Organisationen mit Benutzern betreffen, die sich über eine Vielzahl von tragbaren Geräten und Plattformen aus der Ferne mit einer Vielzahl von in privaten und öffentlichen Rechenzentren gehosteten Apps verbinden.

RISIKOFAKTOR 1

Endgeräte

Die Einführung von tragbaren Geräten in den letzten Jahrzehnten hat unsere Fähigkeit, von überall aus zusammenzuarbeiten und Informationen auszutauschen, stark gefördert. 2020 haben die meisten Unternehmen die Remote-Vollzeitbeschäftigung eingeführt, als ihre Mitarbeiter aufgrund von COVID-19 gezwungen waren, ins Homeoffice zu wechseln.

Wenn auch nicht in allen Fällen, verlief dieser Wechsel in einigen Unternehmen reibungslos, besonders in jenen, die bereits eine Form der mobilen Beschäftigung für Vollzeitkräfte oder der sporadischen Arbeit im Homeoffice unterstützten.

In vielen Fällen musste die IT-Abteilung zügig harte Entscheidungen treffen, wie z. B. welche Geräte berechtigt sind, auf vertrauliche Geschäftsdaten zuzugreifen, und welche ausgeschlossen werden sollten. Das hat zu beachtlichen Unstimmigkeiten geführt, die bestimmte IT- und Sicherheits-Teams nicht vorhersehen konnten.

Mehr Geräte + mehr Gerätetypen

In den letzten 10 Jahren haben Nutzer über ihre Smartphones auf immer mehr Daten aus dem Internet zugegriffen. Das Gleiche gilt für arbeitsbezogene Daten aufgrund des Anstiegs der mobilen SaaS-Anwendungen, einschließlich Produktivitätssuites wie Microsoft Office 365 und CRM Tools wie Salesforce. Aktuell sind 60 % der Geräte, die in einem typischen Unternehmen auf Unternehmensdaten zugreifen können, Mobilgeräte.

Vor 2020 handelte es sich bei mobiler Arbeit im Wesentlichen um ein paar ausgewählte Außendienstmitarbeiter, die über ihr Smartphone in Verbindung blieben, wobei dieses entweder dem Mitarbeiter gehörte (BYOD) oder von der Organisation bereitgestellt wurde (COPE). Jetzt sind es vielmehr Mitarbeiter, die zu Hause oder in einer Ferienwohnung an beliebigen Geräten arbeiten, je nachdem welches Gerät sie gerade zur Hand haben, und offenbar steht ihnen da einiges zur Auswahl. Cisco prognostiziert, dass die Anzahl der mit IP-Netzwerken verbundenen Geräte 2023 auf mehr als das Dreifache der Weltbevölkerung ansteigen wird.

Die Differenzierung zwischen ‚mobilen' Mitarbeitern und Vollzeitkräften im Homeoffice wird mittlerweile immer deutlicher. In dem Zusammenhang verdeutlicht sich auch, dass viele Workflows, an denen die Mitarbeiter arbeiten, sich nicht mit herkömmlichen Tools für die mobile Arbeit vom Homeoffice aus unterhalten lassen oder langfristig tragbar sind.

Ohne das nötige Budget oder die entsprechende Lieferkette, um alle Benutzer mit den passenden Geräten zu versorgen, lassen viele IT-Teams den Kauf eigener Geräte durch die Mitarbeiter zu. Mitarbeiter sind sogar häufig in der Lage, ihren eigenen Rechner und andere Geräte zu kaufen, um ihren Arbeitsplatz zu Hause vollständig einzurichten. Dazu zählen ultra-tragbare, konvertierbare Designs mit enormer Rechenleistung, wie z. B. Surface Pro, oder ein Tablet mit großem Display, das als zweiter Bildschirm fungiert, oder ein Macbook Pro mit einem oder zwei hochauflösenden Bildschirmen. Mitarbeiter, die sich bisher auf einen Festnetzanschluss verlassen haben, haben sich möglicherweise ein zweites Smartphone angeschafft, um Arbeit und Privatleben voneinander zu trennen. Die Auswahl der Gerätetypen ist schier unbegrenzt, und IT-Teams haben alle Hände voll zu tun.

Tele-Mitarbeiter vertrauen zudem auf neue tragbare Internetgeräte, mit denen sie kabellose Geräte über Funksignal verbinden können, wenn die Bandbreite ihres WLAN-Anschlusses zu Hause ausgelastet ist. Dabei kommen Verizon Jetpacks, mobile Hotspots und Mi-Fis für mehrere portable Netzwerkoptionen zum Einsatz, um zuverlässige Internetverbindungen im gesamten Wohnbereich und darüber hinaus aufrechtzuerhalten.

28 %

2020 waren 28 % der Organisationen von einem Betriebssystem mit einer bekannten Sicherheitslücke betroffen.

Durchschnittliche Version des Betriebssystems, OSS- und Gerätemodelle

< 500 Geräte		> 500 Geräte
11.3	Verschiedene Betriebssystemversionen	39.4
1.4	Verschiedene OSS	1.6
1.8	Verschiedene Gerätemodelle	2.6

Im Durchschnitt führen Unternehmen mit < 500 Geräten 11,3 unterschiedliche Versionen von 1,4 verschiedenen Betriebssystemen auf 1,8 unterschiedlichen Gerätemodellen aus. Im Vergleich dazu führen Unternehmen mit > 500 Geräten 39,4 unterschiedliche Versionen von 1,6 verschiedenen Betriebssystemen auf 2,6 unterschiedlichen Gerätemodellen aus.

Eine breitere Vielfalt von Hardware am Arbeitsplatz bringt eine breitere Auswahl von Software mit sich, und wie in der Sicherheitsbranche weitläufig bekannt ist, birgt Software das Potenzial für Schwachstellen. Viele unserer Kunden unterstützen eine Geräteflotte, auf der Kombinationen aus Android, iOS, Mac und Windows 10 laufen. Sie sind bemüht, eine durchgängige Richtlinie für alle Plattformen zu standardisieren, was nicht einfach ist, wenn jede Plattform unterschiedliche Kontroll- und Funktionsebenen sowie unterschiedliche Möglichkeiten für die Vergabe von Sicherheitspatches für gefährdete Betriebssysteme aufweist.

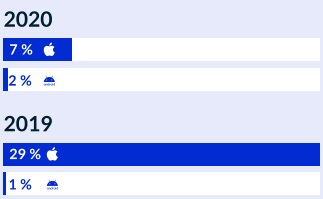
BRANCHENFOKUS

Im Allgemeinen sind Geräte im öffentlichen Sektor aufgrund guter Sicherheitspraktiken weniger Bedrohungen ausgesetzt. Allerdings arbeiten sie häufig mit veralteten Betriebssystemen, wobei im Vergleich mit dem weltweiten Durchschnitt 4,4-mal so viele Benutzer Betriebssysteme mit eher geringfügigen Schwachstellen und 3,6-mal so viele Betriebssysteme mit schweren Schwachstellen betreiben.

Mangel an Gerätestandardisierung ist der neue Standard

Die mangelnde Gerätestandardisierung schafft eine neue Problematik für IT-Teams. Als Organisationen nur mit einem Gerätetyp arbeiteten, wie z. B. einem Windows Desktop-PC, mussten sie sich nur um eine Art Betriebssystem kümmern. Möglicherweise liefen ein paar Rechner auf einer etwas älteren Version, wie z. B. eine, die seit ihrer Herausgabe zwei- bis dreimal erneuert wurde. Das heißt, IT-Teams brauchten sich nur um vier Betriebssystemversionen kümmern und diese auf Schwachstellen überwachen. Heute werden mehrere Plattformen standardmäßig eingesetzt, so z. B. Mac, Windows, iOS und Android. Wenn wir dann auch noch die veralteten Betriebssystemversionen berücksichtigen, kommen wir statt auf nur vier Betriebssystemversionen auf 16 Versionen. Das Fazit ist also: je mehr zur Auswahl steht, umso stärker müssen wir uns darauf vorbereiten, die Verwaltung zu erweitern, um diese Auswahl zu unterstützen.

Anfällige Betriebssystemversion



Auf 7 % der iOS Geräte und 2 % der Android-Geräte liefen 2020 gefährdete Betriebssystemversionen, verglichen mit 29 % bzw. 1 % im Vorjahr. Dieser starke Rückgang bei anfälligen iOS Versionen lässt sich höchstwahrscheinlich auf die Reihe vielfach besprochener iOS Schwachstellen zurückführen, die 2019 auftraten und iMessage und FaceTime betrafen.

Das Dilemma der Endgerätesicherheit

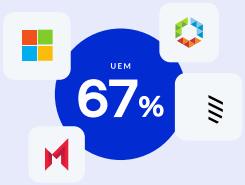
Unternehmen streben eine starke Endgerätesicherheit an, stehen aber häufig vor einem Dilemma, z. B. der Frage, wie sie die Geräte der Vertragspartner vorübergehend sichern, während diese Zugriff auf vertrauliche Daten haben, oder wie sich die Privatsphäre der Mitarbeiter auf BYOD-Geräten bewahren lässt und gleichzeitig ein gewisses Maß an Sicherheit umgesetzt werden kann. Benutzer lehnen Sicherheits- und Verwaltungslösungen im Allgemeinen ab. Sie wollen nicht beobachtet werden und sie wissen, dass diese Lösungen Überwachungen durchführen müssen, um Verdachtsfälle zu erkennen.

Wir wissen, dass 70 % der erfolgreichen Verstöße auf Endgeräten entstehen. Auch wissen wir aus der Aussage von 83 % der Organisationen, dass die Zugriffsbereitstellung an Dritte (z. B. Auftragnehmer oder Lieferkettenpartner) sich schwierig bis sehr schwer gestaltet. Es gibt also einen Verbesserungsbedarf, wenn es darum geht, nicht verwaltete Endgeräte zu sichern.

Laut Verizon beobachten 87 % der Unternehmen, dass die Anzahl der Bedrohungen für Mobilgeräte alle anderen Bedrohungsarten übertrifft. Das lässt sich wahrscheinlich darauf zurückführen, dass Mobilgeräte aufgrund ihrer Personenbezogenheit schwer verwaltet und gesichert werden können, und zwielichtige Akteure sind sich dieser Sicherheitslücke bewusst.

In einer Studie verliehen 92 % der FT 500 Unternehmen ihrer Sorge Ausdruck, dass die wachsende Anzahl ihrer mobilen Mitarbeiter ein zunehmendes Sicherheitsrisiko darstellt. Während die meisten Organisationen verstärkt auf Bring-your-own-Device-Möglichkeiten (BYOD) umgestiegen sind, gab die große Mehrheit (94 %) an, dass BYOD die Risiken für ihre Mobilitätssicherheit erhöht hat.

Fernarbeit dürfte aller Wahrscheinlichkeit nach ein fester Bestandteil der Geschäftspraxis bleiben, selbst wenn ausreichende Anteile der Bevölkerung gegen COVID-19 geimpft wurden. Daher müssen IT-Teams Vorgehen entwickeln, die zu den Anforderungen eines breiten Spektrums aus verwalteten und nicht verwalteten Geräten und Netzwerken passen. Sie müssen auch sicherstellen, dass Remote-Geräte nicht mehr an der Peripherie des Sicherheitsbetriebs verweilen, indem sie die Daten über Bedrohungen von allen Endgeräten in der SOC sammeln.



Laut unseren Daten sind 67 % der Mobilgeräte bei einer Geräteverwaltungssoftware registriert wie z. B. MobileIron oder VMware Workspace ONE.

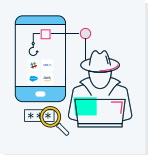
RISIKOFAKTOR 2

Benutzer

In ihrer Entwicklung sind Betriebssysteme dafür ausgelegt, die Mehrheit der Sicherheitsbedrohungen zu mindern. Apple und Google haben viel unternommen, um die Sicherheit ihrer Betriebssysteme und App Stores zu verbessern. Allerdings können Risiken auch durch das Nutzerverhalten einfließen. Für einen Einblick in die Risiken durch Benutzer müssen wir uns ansehen, wie bestimmte Angriffe die Schwächen der Anwender ausnutzen. Aber wir müssen auch Nutzerverhaltensweisen berücksichtigen, die die Sicherheit der Geräte schwächen und somit die Tür zum Angriff öffnen.

Benutzer als gezieltes Opfer

Hacker umgehen immer noch verstärkte Betriebssysteme mit Social-Engineering-Angriffen wie Phishing, das es darauf anlegt, den Benutzer zur Übergabe vertraulicher Informationen zu bewegen. Der Datenverkehr kann zudem von böswilligen Akteuren abgefangen werden, die den unsicheren Status eines öffentlichen WLANs nutzen. Zudem fallen einige Benutzer auf zweifelhafte Apps herein, die einen Datenverlust verursachen, wie z. B. PII oder Gelddiebstahl oder anderer Scam-Betrug.

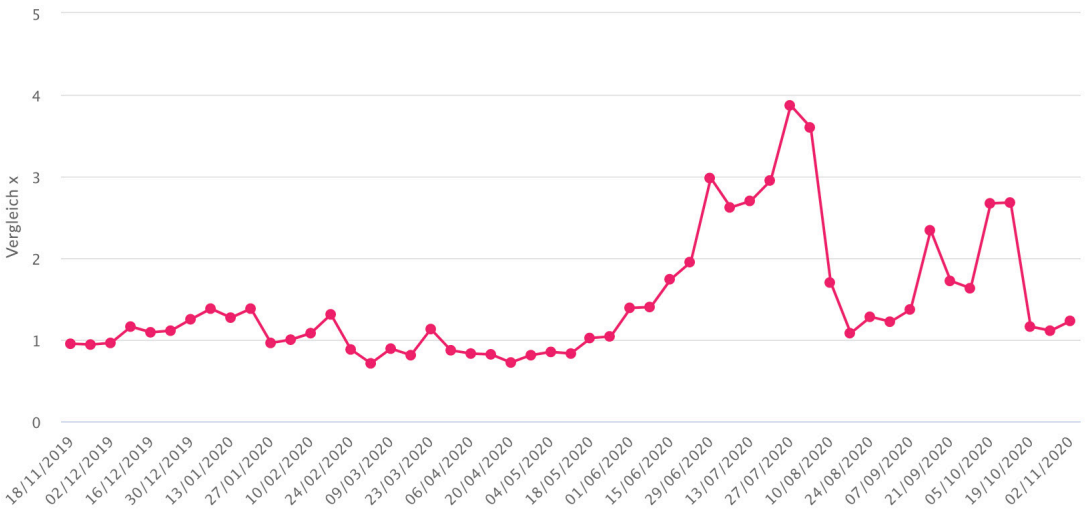


BENUTZER ALS GEZIELTES OPFER

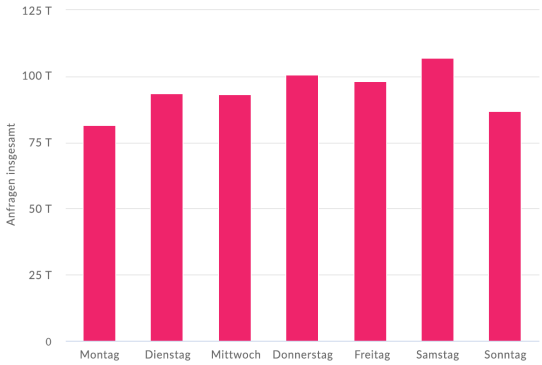
Phishing

Phishing bleibt die häufigste Bedrohung, von der Benutzer von Mobilgeräten betroffen sind. Phishing-Angriffe zielen normalerweise auf ein bestimmtes Thema, eine Produktmarke oder ein Motto ab, die oder das die Aufmerksamkeit der Opfer erregt. So gibt es im Zeitraum der Steuerabrechnungen in der Regel einen Anstieg an Phishing-Angriffen, bei denen der Angreifer sich als das Finanzamt ausgibt. Ebenso haben wir in der ersten Hälfte dieses Jahres einen Anstieg des Datenverkehrs zu COVID-19-bezogenen Phishing-Websites bemerkt, und es trat sogar eine gefälschte E-Commerce-Site von Clorox auf.

Das folgende Diagramm zeigt die Zunahme der Phishing-Angriffe, die im Laufe des Jahres 2020 auf Telearbeiter abzielten.



Auf der Suche nach anderen Phishing-Trends, die 2020 entstanden sind, bemerkten wir, dass Phishing-Angriffe die Benutzer am häufigsten an einem Samstag erreichen. Phishing-Angriffe traten zu Spitzenzeiten an Wochenenden um 6 % häufiger auf als zu Spitzenzeiten während der Arbeitstage. Das stärkt die Vermutung, dass Mitarbeiter im Freizeitmodus auf ihren Unternehmensgeräten eher für Phishing anfällig sind, da sie entspannt sind.



BENUTZER ALS GEZIELTES OPFER

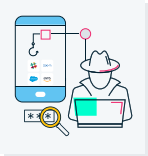
Man-in-the-Middle-Angriffe auf WLAN

Bei einem Man-in-the-Middle-Angriff (MitM) stellt das WLAN ein schwerwiegendes Datenschutzrisiko dar. Es gibt zwei Hauptansätze eines MitM-Angriffs, die Mobilgerätenutzer betreffen. Beim ersten Ansatz verschafft sich der Angreifer physische Kontrolle über die Netzwerkinfrastruktur, z. B. über einen gefälschten WLAN-Zugriffspunkt, und kann den durchgehenden Datenverkehr aufspüren. Der zweite Ansatz erfolgt über die Manipulation des der Verschlüsselung dienenden Netzwerkprotokolls durch den Angreifer, sodass Daten freigegeben werden, die geschützt sein sollten. Alarmierend ist dabei, dass mehr als 80 % der Mitarbeiter für Arbeitsvorgänge ein öffentliches WLAN nutzen, selbst wenn ihnen dies offiziell untersagt ist.

> Im Jahr 2020 haben sich 4 % der Benutzer jede Woche mit einem riskanten Hotspot verbunden – im Vergleich zu 7 % im Jahr 2019.

Sehen wir uns an, wie sich die Auswirkungen der WLAN-Bedrohungen, inklusive MitM-Angriffe, im Laufe des Jahres 2020 geändert haben.

Als wir diese Analyse durchführten, erwarteten wir aus offensichtlichen Gründen einen Rückgang, da Personen nicht so häufig zur Arbeit pendelten, wie sie dies vor Ausbruch von Pandemie taten (ca. Februar bis März 2020). In diesem Diagramm sehen wir einen kurzen Anstieg im Januar, als die Menschen wieder zur Arbeit zurückkehrten und dann einen starken Rückgang im Februar, als die COVID-19-Fallnummern stark anstiegen und Unternehmen Geschäftsreisen stornierten und die Mitarbeiter aufforderten, im Homeoffice zu arbeiten, wo sie sicherer waren.



BENUTZER ALS GEZIELTES OPFER

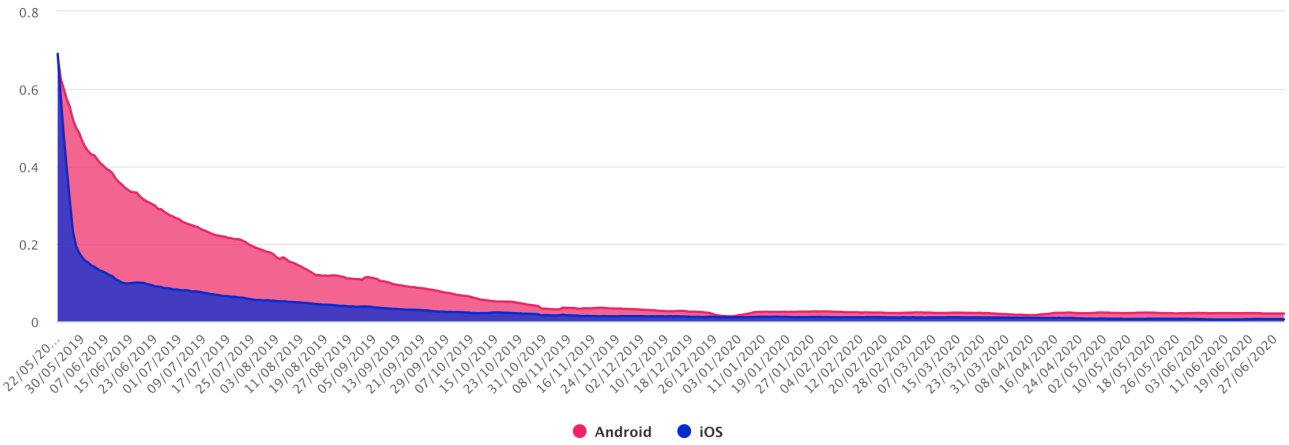
Risiken von Apps

Schädliche Apps, wie Malware, setzen zunehmend ausgeklügeltere Techniken ein, um nicht erkannt zu werden. So wartet raffinierte Malware beispielsweise eine Reihe von Schritten ab, bevor sie bösartiges Verhalten initiiert, z. B. verhält sie sich nur in einem bestimmten Netzwerk schädigend, oder sie enthält ruhenden Command-and-Control-Code, der jederzeit vom Hacker aktiviert werden kann. Grundlegende Prüfungen, wie jene von den App-Stores, können ausgeklügelte, aber überraschend häufig auftretende böswillige Apps nicht erkennen.

> Im Jahr 2020 erlitten 52 % der Organisationen einen Malware-Vorfall auf einem Remote-Gerät – eine Steigerung im Vergleich zu 37 % im Jahr 2019.

Abgesehen davon, dass Malware in Anwendungen versteckt sein kann, ist es auch möglich, dass Apps von den Entwicklern schlecht entwickelt, gesichert oder gewartet werden, und daher gefährliche Schwachstellen aufweisen, wie die 2019 und 2020 in WhatsApp erkannten Lücken.

> Android-Nutzer verzögerten die Aktualisierung ihrer Apps, nachdem im Mai 2019 eine bedeutende Schwachstelle in einer älteren Version von WhatsApp erkannt worden war, wie in diesem Diagramm ersichtlich. Etwa 85 % der verbleibenden Geräte mit der betroffenen WhatsApp-Version wurden zwischen Mai und Mitte Juli 2019 aktualisiert. Im Vergleich dazu wurden nur etwa 50 % der betroffenen Android-Geräte in diesem Zeitraum aktualisiert.



Manchmal beinhalten Apps einen Scam oder eine andere betrügerische Handlung, und häufig fügen die Entwickler diesen Betrug über die Infrastruktur von werbetreibenden Drittanbietern hinzu. Wir haben Apps gesehen, die die offizielle App Store-Prüfung bestanden haben, obwohl sie dauernd Pop-Up-Anzeigen anzeigten, die das Geräte-Display in Beschlag nahmen, wodurch es unbrauchbar wurde. Diese von uns als potenziell unerwünscht bezeichneten Apps lassen sich auf jedem 200. Gerät finden.

Einige Entwickler gehen vielleicht sogar so sorglos vor, ganz auf Verschlüsselung zu verzichten, und setzen Benutzer (und auch deren Arbeitgeber) einem Datenverlust aus.

- 2020 wiesen 15 % der Organisationen mindestens ein Gerät mit einer App auf, die Passwortdaten freigab, eine Steigerung gegenüber 11 % aus dem Vorjahr.
- Im Jahr 2020 waren iOS Geräte 3,2-mal eher von Datenleck-Anwendungen betroffen als Android-Geräte

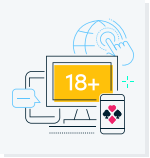
Unsere kürzlich erstellte Analyse zeigt, dass, sobald ein Risiko von einer nicht zugelassenen Anwendung eingeführt wurde, dieses Risiko zunimmt.

- wobei alle Unternehmen, in denen mindestens ein Gerät durch Malware kompromittiert wurde, 4,4-mal häufiger von einer Passwortfreigabe betroffen sind als andere Unternehmen.
- sind durch Installation einer gefährdenden Anwendung 59-mal häufiger von kryptografischem Hijacking-Verkehr betroffen als andere Nutzer.

Eine unabhängige Sicherheitsprüfung der Anwendung ist aufwändig, aber eine notwendige Aufgabe. Da wir heute mehr Geräte als jemals zuvor verwenden, haben Benutzer Zugriff auf eine Vielzahl von Anwendungen. Dies geschieht jedoch nicht immer mit böser Absicht. So möchte ein Benutzer vielleicht ein Tool zum Zusammenfügen von PDF-Dateien oder ein anderes Dateimanagement-Tool verwenden, das von der IT nicht genehmigt wurde, aber diese App ist möglicherweise risikobehaftet. Die IT-Abteilung muss sich aus zweierlei Gründen bewusst sein, welche Apps die Mitarbeiter für ihre Arbeit wählen: (1) sie muss einer Risikoprüfung unterzogen werden, und (2) sie muss auf ihren produktiven Nutzen bewertet werden, und wenn sie auf sichere und gute Weise zur Produktivität beiträgt, sollte ihrer Genehmigung und ihrem Schutz nichts im Wege stehen.

Benutzer als verantwortlich für fehlerhafte Entscheidungen

Im vorherigen Abschnitt haben wir uns Risiken angesehen, die Benutzer, wenn auch passiv, initiieren. In diesem Abschnitt geht es um Risiken, die von einer aktiveren Rolle des Benutzers ausgehen, d. h. wenn Benutzer die Unternehmensrichtlinien und vorhandenen Sicherheitsmaßnahmen gezielt umgehen. Für Benutzer können nach unachtsamen Entscheidungen Probleme entstehen, beispielsweise wenn sie auf nicht konforme Inhalte zugreifen oder in die Gerätesicherheit eingreifen, indem sie Geräte per Jailbreak freischalten, Anwendungen im „Sideloading" Verfahren laden oder Bildschirmsperren deaktivieren.

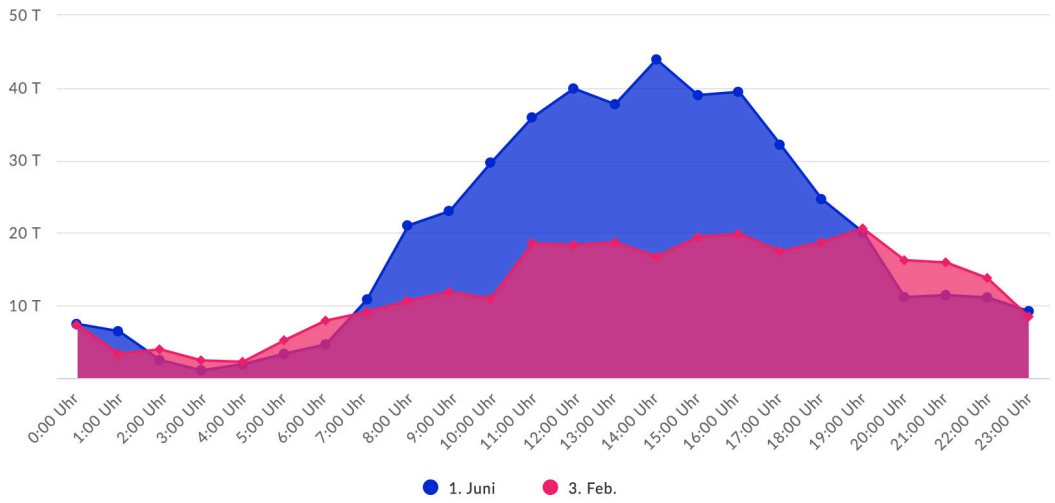


BENUTZER ALS VERANTWORTLICH FÜR FEHLERHAFTE ENTSCHEIDUNGEN

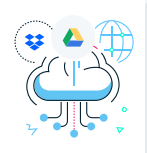
Unangemessener Inhalt

Mit Geräten in Ihrer IT-Infrastruktur, die Zugang zu den dunkelsten Ecken des Internets haben, gehen Sie ein geschäftsweites Risiko ein. Wenn wir von unangemessenen Inhalten sprechen, sind damit Kategorien gemeint, die nicht für Minderjährige geeignet sind, u. a. Glücksspiele, extreme und illegale Inhalte, bei denen die Wahrscheinlichkeit eines Datenlecks sehr viel höher ist, die unverschlüsselte Technologien einsetzen und Organisationen anderweitig Risiken aussetzen. Erstaunlicherweise greifen viele Nutzer mit ihren Arbeitsgeräten auf die zwielichtigen Teile des Internets zu.

Verglichen mit der Zeit vor Beginn der Pandemie stieg die Anzahl der Aufrufe unangemessener Inhalte während der Arbeitszeit um bis zu 100 %. Wenn Beschäftigte aus dem Homeoffice arbeiten, besteht die eindeutige Notwendigkeit, dafür zu sorgen, dass sie auf ihren zur Fernarbeit genutzten Geräten akzeptable Nutzungsrichtlinien einhalten.



Content-Filter sind eine wirksame Möglichkeit, die Einhaltung akzeptabler Anwendungsrichtlinien im Unternehmen für eine Bandbreite von Endgeräten durchzusetzen, um Sicherheit, Compliance und rechtliche Risiken für Arbeitnehmer wie auch Arbeitgeber zu mindern.



BENUTZER ALS VERANTWORTLICH FÜR FEHLERHAFTE ENTSCHEIDUNGEN

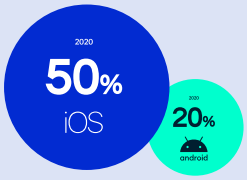
Umgehung von Sicherheitsmaßnahmen

Schwachstellen sind nicht ausschließlich etwas, was Benutzern zustößt, sondern Benutzer können ihre Geräte manchmal auch vorsätzlich oder unbeabsichtigt anfällig machen.

Jailbreaking

Jailbreaking und Geräte-Rooting sind riskante Konfigurationen, die es Benutzern ermöglichen, auf das Betriebssystem eines Geräts zuzugreifen und die Installation von nicht autorisierten Softwarefunktionen und Anwendungen zu aktivieren. Diese Taktiken sind zudem bei Benutzern beliebt, die ihr Gerät von einer Betreibersperre befreien möchten.

- Im Jahr 2020 stieg die Anzahl der im Jailbreak-Verfahren geänderten iOS Geräte um 50 % an, und die Anzahl der Root-veränderten Android-Geräte stieg um 20 %.
- Per Jailbreak veränderte Geräte sind 28-mal häufiger von böswilligem Netzwerkdatenverkehr betroffen als intakte Geräte.
- Unternehmen, die in ihrer Flotte mindestens ein im Jailbreak-Verfahren geändertes Gerät haben, sind auf ihren Geräten 31,6-fach häufiger schädlichem Netzwerkverkehr ausgesetzt als andere Unternehmen.
- Auf derart veränderten Geräten wurde mit 33-facher höherer Wahrscheinlichkeit eine Anwendung mit einer bekannten Schwachstelle installiert als bei unveränderten Geräten.



Im Jahr 2019 stieg die Anzahl der im Jailbreak-Verfahren veränderten iOS Geräte um 50 % an, und die Anzahl der Root-veränderten Android-Geräte stieg um 20 %.

Sideloading von Apps

Während einige iOS Benutzer ihre Mobilgeräte möglicherweise gezielt per Jailbreak „knacken“, um Sicherheitsverbesserungen zu installieren, tun die meisten Benutzer es, um Anwendungen zu installieren, die in den offiziellen App-Stores nicht angeboten werden. Auch ist es möglich, Apps von Drittanbietern zu installieren, ohne dass das Gerät dazu im Jailbreak-Verfahren geändert werden muss; dieser Prozess wird als Sideloading von Apps bezeichnet. Dazu muss der Benutzer das Gerät lediglich so konfigurieren, dass es einem spezifischen Entwickler vertraut, um dann jede beliebige App von diesem Entwickler zu installieren, ohne vorher den App-Store aufzurufen. Viele Unternehmen gehen so vor, um Apps auf den Geräten ihrer Mitarbeiter zu installieren, ohne diese Apps zuvor im App Store veröffentlichen zu müssen.

Google sperrt das Android-Betriebssystem nicht in dem Maße, wie Apple dies mit iOS tut. Obwohl die Standardkonfiguration von Android-Geräten kein Sideloading von Apps zulässt, kann die Einstellung so verändert werden, dass Apps von Drittanbietern zugelassen werden. Laut unseren Daten hat jeder fünfte Android-Benutzer seine Geräte so konfiguriert, dass App-Installationen von Drittanbietern möglich sind.

Benutzer, die Apps im Sideload-Verfahren laden, sind erhöhten Sicherheitsrisiken ausgesetzt, da der von Apple und Google in ihren offiziellen App Stores durchgeführte Prozess der Anwendungsprüfung umgangen wird, und das Gerät daher in geringerem Maße vor unbeabsichtigt installierter Malware geschützt ist.

Im Jahr 2020 enthielt jedes zehnte Android-Gerät, das für die Arbeit verwendet wird, einen App-Store eines Drittanbieters (d. h. einen anderen Shop als Google Play).

BRANCHENFOKUS – RECHTSWESEN

Im juristischen Bereich verwenden Benutzer mit 2,5-facher größerer Wahrscheinlichkeit im Sideload-Verfahren installierte Anwendungen auf ihren Geräten als in anderen Branchen.

BRANCHENFOKUS – FERTIGUNG

In der Fertigungsbranche sind Geräte doppelt so häufig Malware ausgesetzt als in anderen Branchen. Das kann im Zusammenhang damit stehen, dass 50 % mehr Benutzer App-Stores von Drittanbietern installiert haben und Android-Benutzer doppelt so häufig unbekannte Quellen aktiviert haben.

Deaktivierung der Bildschirmsperre

Erstaunlicherweise wird eine der einfachsten Sicherheitsmaßnahmen auf einem Mobilgerät immer noch ignoriert: die Bildschirmsperre. Obwohl die Bildschirmsperre in den meisten Geräten standardmäßig aktiviert ist, versuchen einige Benutzer alles, um sie zu deaktivieren, wodurch ihre Geräte bei physischem Diebstahl viel anfälliger sind. Es ist zudem ein Hinweis auf generell schlechte Sicherheitspraktiken. Unsere Daten haben gezeigt, dass auf Geräten, auf denen diese einfache Sicherheitsmaßnahme entfernt wurde, die Bedrohungen zunehmen.

- 2020 war auf 3 % der für die Arbeit verwendeten Geräte die Bildschirmsperre deaktiviert worden, ein geringerer Anteil als 6 % im Jahr 2019.
- Benutzer, die ihre Bildschirmsperre deaktivieren, führen 16-mal häufiger als andere Benutzer ein Betriebssystem mit einer bekannten Schwachstelle aus.
- Benutzer, die ihre Bildschirmsperre deaktiviert haben, laufen 2,4-mal häufiger Gefahr, ihre E-Mail-Adresse an Angreifer freizugeben, als andere Benutzer.

BRANCHENFOKUS – IT-DIENSTLEISTUNGEN

Im globalen Durchschnitt haben Benutzer im IT-Bereich die Bildschirmsperre auf ihren Geräten 2,2-mal häufiger deaktiviert.

2020 war auf 3 % der für die Arbeit verwendeten Geräte die Bildschirmsperre deaktiviert worden, ein geringerer Anteil als 6 % im Jahr 2019.

RISIKOFAKTOR 3

Fernzugriff

Wir haben uns bisher Risiken für das Gerät und Betriebssystem sowie vom Benutzer initiierte Risiken angesehen, aber wie sieht es eigentlich mit dem Risiko dieser Faktoren für vertrauliche Unternehmensanwendungen aus, wenn der Fernzugriff unsachgemäß konfiguriert oder überhaupt nicht gesichert ist? Welche Schutzvorrichtung sollte zwischen dem risikobehafteten Gerät oder dem risikofreudigen Benutzer und den vertraulichen Daten in Unternehmensanwendungen bestehen?

Was den Schutz von Unternehmensanwendungen betrifft, geht es nicht um Anwendungsschutz oder Mobile Application Management (MAM), sondern um den sicheren Zugriff auf vertrauliches geistiges Eigentum in diesen Anwendungen und Workloads, die in der Cloud laufen.

Laut dem Cybersecurity Insiders Remote Workforce Security Report 2020 erlauben 65 % der Organisationen es ihren Mitarbeitern, von privaten, nicht verwalteten Geräten auf verwaltete Anwendungen zuzugreifen.

Darüber hinaus zeigt der IDC-Bericht ‚Remote Access and Security Challenges & Opportunities' auf, dass 40 % der Cyber-Sicherheitsverstöße durch den Zugriff autorisierter Benutzer auf nicht autorisierte Systeme entstehen.

Viele geschäftliche Anwendungen an vielen Orten

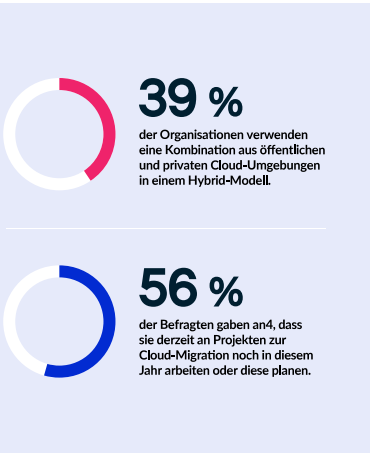
Eins lässt sich in der Sicherheitsbranche mit Bestimmtheit sagen: die befragten IT-Fachkräfte schweben in der Cloud. Laut den Umfragedaten aus dem Cloud Adoption in 2020 Report von O'Reilly's verwenden 39 % der Organisationen eine Kombination aus öffentlicher und privater Cloud in einem Hybrid-Modell. Darüber hinaus gaben in dieser Umfrage mehr als 56 % der Befragten an, dass sie aktuell an Cloud-Migrationsprojekten arbeiten oder sie in diesem Jahr planen.

Aus diesen Daten lässt sich ablesen, dass viele Organisationen im Begriff sind, eine dezentralisierte, hybride Umgebung einzurichten, oder dies bereits getan haben, in der die Daten in einer diversifizierten Infrastruktur lagern. Einige werden bestimmte Anwendungen unbefristet weiter kontrollieren, aber Cloud- und SaaS-Lösungen machen es möglich, Anwendungen außerhalb des Unternehmensbereichs einzusetzen, wodurch der Anwendungszugriff zu einem kritischen Thema für Sicherheitsdienstleister wird.

An vielen modernen Arbeitsplätzen werden cloudbasierte Anwendungen bevorzugt, da deren Bereitstellung, Verwaltung und Pflege für das Unternehmen einfach und kosteneffizient ist. Öffentliche wie auch private Cloud-Dienste weisen eine akzeptable Erfolgsbilanz auf und stellen somit eine sinnvolle Lösung für Unternehmen jeder Größe dar. Ebenso werden SaaS-Lösungen für bestimmte Anwendungen bevorzugt, da sie die Unternehmen komplett von der Aufgabe der Entwicklung und vom Wartungsaufwand befreien. Die Vorteile überwiegen zweifellos die Risiken, was SaaS betrifft, denn warum sollte man einen Brunnen graben, wenn der Wasserhahn es auch tut? Gartner zufolge konnten SaaS-Lösungen allein im Jahr 2020 einen Umsatz von etwa 105 Milliarden US-Dollar generieren.

Da viele Organisationen einige Apps in die Cloud verschieben und die Anzahl der von ihnen verwendeten SaaS-Anwendungen erweitern, verwalten sie mehr Anwendungen an mehr Standorten als je zuvor. Gemäß Okta gilt auch: je größer die Organisation, desto mehr Anwendungen möchte sie nutzen.

Die Anzahl der Software-Apps, die große Unternehmen aller Branchen weltweit bereitgestellt haben, ist im Laufe von vier Jahren um 68 % gestiegen, was laut einer Analyse von Okta einen Durchschnitt von 129 Apps pro Unternehmen bis Ende 2018 ergibt. Fast 10 % der Unternehmen verwendeten zum Zeitpunkt der Umfrage mehr als 200 Anwendungen.



Die Notwendigkeit des modernen Fernzugriffs

Vormals versuchten Unternehmen nur eins zu schützen, ihr Rechenzentrum, das sie physisch abriegelten. Veraltete Tools für den Fernzugriff wie VPN und RDI gingen von der Basis der Unternehmenszentrale aus und boten eine adäquate Funktion für Anwendungen, die vom Rechenzentrum aus betrieben wurden. Bei einem derartigen Burg- oder Festungsmodell wird Vertrauen auf alle im Netzwerk gesetzt. Das bedeutet, dass potenzielle Angreifer auf ganze Netzwerksegmente zugreifen können, da VPNs und RDIs ohne eine konsequente Verifizierung der Benutzeridentität oder des Sicherheitsstatus des Geräts implizit Verbindungen „vertrauen".

Laut IDC wurde bei 68 % der schwersten Vorfälle mit Tools zum Fernzugriff ein VPN verwendet. Des Weiteren gehen 40 % der Cybersicherheitsverstöße von autorisierten Benutzern aus, die auf nicht autorisierte Systeme zugreifen.

Warum sind kontinuierliche Risikobewertungen ein wichtiger Teil einer Strategie zur Überwachung des Fernzugriffs? Werfen wir dazu einen Blick auf die Zahlen.

- Von einem von 83 Geräten, auf denen 2020 ein gefährdetes Betriebssystem lief, wurde zum Zeitpunkt der bestehenden Sicherheitslücke E-Mail abgerufen, und jedes sechste Gerät griff auf den Cloud-Speicher zu.
- Von den 2020 durch Malware kompromittierten Mobilgeräten griffen 37 % nach der Kompromittierung weiter auf E-Mail-Nachrichten des Unternehmens und 11 % weiter auf den Cloud-Speicher zu.
- In 42 % der Unternehmen mit von Malware betroffenen Geräten griff mindestens eines der kompromittierten Geräte auf Produktivitäts-Tools zu.
- Auf jedem 200. Gerät mit Zugriff auf den Cloud-Speicher war die Bildschirmsperre deaktiviert.
- In mehr als 40 % der Unternehmen mit Benutzern, die mit anfälligen Betriebssystemen arbeiten, wird von mindestens einem der gefährdeten Geräte auf den Cloud-Speicher zugegriffen.
- 1,3 % der Kunden verwenden ein durch Malware kompromittiertes Gerät, von dem aus auf Produktivitäts-Tools wie Office 365 und Google Workspace zugegriffen wird.
- Wir wissen, dass vertrauliche Geschäftsdaten nicht allein durch Benutzerauthentifizierung vor kompromittierten Geräten geschützt werden können. Wie sieht die Lösung aus? Zero Trust Network Access ist ein grundlegend neuer Ansatz im Vergleich zum herkömmlichen Ansatz. Schluss mit Kästen, Ausstattung oder physischen Geräten. Entscheidend ist zudem, dass Netzwerksicherheit aus der Cloud skalierbar ist. Ohne diese Option wäre es Ihnen gar nicht möglich, genug Ausstattung zu kaufen, um alle Daten beim Wechsel von der Unternehmenszentrale in die Cloud zu schützen.

Zusätzlich kann Zero Trust Network Access auf den Geräten fortlaufende Risikobewertungen durchführen, die Zugriff auf Ihre vertraulichen Anwendungen anfordern, um sicherzustellen, dass das Gerät konform ist, und dazu zählen unter anderem, dass es sich in einem guten Netzwerk am erwarteten Standort befindet und frei von Infektionen und Sicherheitslücken ist, und dass der Benutzer zur jeweiligen Abfrage berechtigt ist.

42 %

der Unternehmen, deren Geräte von Malware betroffen waren, geben an, dass mindestens eines der kompromittierten Geräte auf Produktivitäts-Tools zugreift.

Von einem von 83 Geräten, auf denen 2020 ein gefährdetes Betriebssystem lief, wurde zum Zeitpunkt der bestehenden Sicherheitslücke E-Mail abgerufen, und jedes sechste Gerät griff auf den Cloud-Speicher zu.

CLOUD-SICHERHEITSBERICHT

Empfehlungen

Trotz jahrzehntelanger Bemühungen seitens Unternehmen, ihre IT-Standards zu definieren, ist mittlerweile in vielen Unternehmen der Mangel an Standardisierung zum Standard geworden. Welches Betriebssystem verwendet Ihr Unternehmen? Alle. Welche Benutzer haben berechtigten Zugriff auf Ihre Anwendungen? Alle. An welchen Standorten dürfen Benutzer arbeiten? An beliebigen Standorten.

Sichere Fernzugriffslösungen müssen ausreichend flexibel und agil sein, um die Arbeit zu ermöglichen, ohne sie zu blockieren oder die Produktivität einzuschränken. Zur Entwicklung einer modernen SASE-Sicherheitsstrategie, die zu modernen IT-Umgebungen passt, empfehlen wir den Einsatz dieser Checkliste.

Halten Sie die Anforderungen auf Grundlage der neuen Einsatzbereiche, die aus der Fernarbeit entstehen, fest.

- Wozu sollen die Mitarbeiter an ihren Geräten in der Lage sein: auf E-Mail oder auf vertrauliche Datenbanken zuzugreifen? Segmentieren Sie die Daten, damit der Zugriff auf Detailebene erfolgen kann.
- Beurteilen Sie die Einsatzbereiche und definieren Sie die Anforderungen für Ihre Mitarbeiter im Homeoffice.
- Die obigen Anforderungen haben Auswirkungen auf das Eigentumsmodell Ihrer Geräte: Welche Gerätetypen werden Sie unterstützen, wer wird sie besitzen und wie werden sie verwaltet?

Konnektivität

- Legen Sie bezüglich Konnektivität und Cloud-Anwendungen fest, was Sie über Benutzer, Geräte, Netzwerke und Apps wissen müssen, bevor Sie ihnen Zugriff auf Unternehmensressourcen gewähren.
- Beschränken Sie die Business-Tools, die die Benutzer brauchen, um zu verhindern, dass Konten mit unzähligen Berechtigungen für einen Angriff auf eine große Anzahl von Systemen missbraucht werden.

Definierung des akzeptablen Gebrauchs

- Überprüfen Sie die vorhandenen Richtlinien für den akzeptablen Gebrauch und stellen Sie sicher, dass alle Endgeräte erfasst sind.
- Implementieren Sie Richtlinien für den akzeptablen Gebrauch für jede Untergruppe von Geräten, um eine Schatten-IT und unerwünschte Nutzung zu verhindern und für die Beachtung der geltenden Vorschriften zu sorgen.

Erweiterung der Richtlinien für die Zugriffsverwaltung zur Aufnahme des Geräterisikostatus

- Implementieren Sie zu Authentifizierungszwecken eine benutzerfreundliche IAM-Lösung (Identity and Access Management), um Anwendungen auf allen Geräten, einschließlich Mobilgeräten, zu erfassen.
- Nehmen Sie Ihre Geräterisikoeinschätzungen in Ihre IAM-Richtlinien auf, um sicherzugehen, dass der Risikostatus des Geräts berücksichtigt wird.
- Stellen Sie sicher, dass der Risikostatus während der Sitzung kontinuierlich beurteilt wird.

Stellen Sie Endgeräteschutz für alle Geräte bereit. Eine cloudbasierte Sicherheitslösung ist besonders für den Schutz vor den vielen verschiedenen Cyberbedrohungen und Anwendungsrisiken von Bedeutung.

- Stellen Sie sicher, dass Ihre Sicherheitslösung über eine starke Endgeräteerkennungsfunktion und eine Architektur im Netzwerk verfügt, um Angriffe zu verhindern, bevor sie das Gerät erreichen.
- Stellen Sie sicher, dass Ihre Sicherheitslösung sowohl externe Cyberbedrohungen (wie Phishing, Man-in-the-Middle-Angriffe, Malware) als auch Risiken durch das Nutzerverhalten (Sideloading usw.) erfasst.
- Stellen Sie für alle Sicherheitstools sicher, dass eine für Ihr Unternehmen angemessene Konfiguration erfolgt, um die Angriffsvektoren angehen zu können und gleichzeitig die Privatsphäre Ihrer Endbenutzer zu respektieren.
- Bewerten Sie die maschinelle Lernkapazität der Sicherheitslösung, um zu erkennen, wie die Bedrohungs-Engine neue Bedrohungen erkennt und davor schützt.

Implementierung einer UEM zur Kontrolle auf Geräteebene

- Implementieren Sie gegebenenfalls eine UEM-Lösung, die es Ihnen ermöglicht, Geräte aus Unternehmensressourcen bereitzustellen und laufende Compliance-Kontrollen des Geräts durchzuführen.

Gehen Sie diese Liste regelmäßig durch und überlegen Sie sich, welche Änderungen aufgrund des folgenden Sachverhalts vorgenommen werden müssen

- Änderungen in der Unternehmensgröße oder Zusammensetzung, wie z. B. Fusionen oder Akquisitionen
- Neue Vorschriften, die die Art der Datenverarbeitung betreffen
- Entwicklung der IT-Strategie
- Bedrohungen, von denen Ihre Mitarbeiter betroffen sind
- Neue Anwendungen, die die Mitarbeiter für ihre Arbeit brauchen