ZIMPERIUM®

Berichtsindex globaler Mobilbedrohungen 2022

With contributions by:

intertrust

Ping Identity

SentinelOne

Inhaltsverzeichnis

Mobile Sicherheit in der aktuellen Zeit

Shridhar Mittal, CEO, Zimperium

Ich muss Ihnen wahrscheinlich nicht erzählen, dass die letzten Jahre die modernen Arbeitsbedingungen auf eine Art und Weise verändert haben, die wir uns vor zehn Jahren noch nicht hätten vorstellen können. Dezentralisierte und hybride Belegschaften, ständig verbundene Geräte, Verbindungen über 5G-Hochgeschwindigkeitsnetze und vermehrte Zugriffe auf kritische Daten von entfernten Standorten haben viele Unternehmen global gemacht. Ich muss sicherlich ebenfalls nicht erwähnen, dass sich die Dinge im Jahr 2022 erneut vollständig anders darstellen werden, als die Jahre 2021 und 2020. Wie wir alle wissen, sind wir aktuell Lichtjahre entfernt von der Art und Weise, wie Arbeit, Kollaboration und Produktivität vor und bis zum Ende des Jahres 2019 ausgesehen haben.

Für Jahrzehnte bauten IT- und Sicherheitsteams Infrastrukturen vor Ort auf, um die dortigen Mitarbeiter zu unterstützen und nur einige wenige Teile der Belegschaft befanden sich außerhalb der Büros. Sicherheit und Dienste wurden implementiert, um eine digitale, schichtweise Festung aufzubauen und so Mitarbeiter, Endgeräte und Daten zu schützen. Doch alte Technologien wie zum Beispiel VPNs wurden nicht dazu entwickelt, diese Masse an externen Verbindungen mit dem Unternehmen zu händeln. Doch als die meisten Mitarbeiter sich nicht länger innerhalb dieser digitalen und physischen Schutzzonen befanden und nachdem die meisten lokal installierten Produktivitätswerkzeuge auf ein „Software als Dienstleistung"-Modell umgestiegen sind, begannen Sicherheitsorganisationen damit, in fortschrittliche Sicherheitskontrollen für Endgeräte und ihre unterstützte Infrastruktur zu investieren.

Zum Glück waren die Motivation und Mentalität zur Bereitstellung sicherer Remote-Kollaboration schon vor COVID-19 bei vielen Unternehmen vorhanden, während global agierende Firmen Mobilität, Remotezugriff, „Zero Trust" und Produktivitätsinitiativen verfolgten. Unternehmen begannen, in cloudbasierte Dienste und Anwendungen zu investieren und bewegten dabei Daten von Speicherservern vor Ort auf skalierbare Lösungen weltweit. Da dieses Fundament bereits gelegt war, wirkte die globale Pandemie eher als Bestätigung und Katalysator statt als eine Unterbrechung ihre Geschäfte. In diesem Kontext waren Flexibilität, Skalierbarkeit und Zugänglichkeit primäre Schlüsselelemente für diese neuen Investitionen. Doch was ist mit der Sicherheit?

Trotz ihrer Bemühungen ist die Realität weiterhin, dass die Arbeitswelt sich schneller weiterentwickelt hat, als diese Teams und Strategien erwartet haben. **Insbesondere in den letzten zwei Jahren haben viele Unternehmen Sicherheitskontrollen geopfert, um die Produktivität und eine fortführung der Geschäftstätigkeiten zu sichern.**

Es muss außerdem erwähnt werden, dass IT- und Sicherheitsfirmen schon immer stark in die Endgerätesicherheit investiert haben, jedoch eine Tendenz besitzen, die potentiellen Auswirkungen der verschwimmenden Linie zwischen mobilen und traditionellen Endgeräten zu unterschätzen.

Laut unseren Daten haben 66 % der vor Kurzem befragten Unternehmen aktive BYOD-Programme („Bring your own Device", also die Verwendung privater Endgeräte) und weitere 11 % planen, diese Richtlinie im Laufe des nächsten Jahres umzusetzen.[1]

Heute verbinden sich mehr denn je vom Unternehmen verwaltete und nicht verwaltete Geräte mit Unternehmensdaten über unbekannte und nicht in Unternehmenshand liegenden Netzwerken. Notwendigerweise müssen Sicherheitsteams jedes Endgerät mit einer völlig neuen Einstellung angehen. All dies beginnt mit der Sichtbarmachung aller mit den Unternehmensystemen verbunden Geräten, unabhängig davon, ob sie vom Unternehmen verwaltet werden oder nicht. Andernfalls arbeiten Sicherheitsteams im Blindflug gegenüber den Bedrohungen und Risiken, die täglich ohne Datenzuweisung und Gerätebeglaubigung aufkommen. Unternehmen benötigen mehr Werkzeuge als nur Mobilgeräte- und Anwendungsverwaltungswerkzeuge und müssen auch die wichtigen Sicherheitsherausforderungen thematisieren, die mobile Geräte mit sich bringen.

Laut unseren Daten sind 10 % der Anwendungen, die auf mobilen BYO-Endgeräten installiert sind, unternehmensbezogen – begonnen bei Multi-Faktor-Authentifizierungen (MFA) über Datenzugriffswerkzeugen bis hin zu Kommunikationsanwendungen.[2]

Während Unternehmen sich weiterentwickeln, beginnen sie auch, mehr Anwendungen zu nutzen, die sich mit kritischen Datensystemen verbinden, um die nun globale Belegschaft zu unterstützen. Dies bedeutet, dass diese neuen Risiken auch über das Mobilgerät an sich hinaus gehen. **Die Angriffsfläche eines Unternehmens wächst mit jeder im Sinne der Produktivität neu eingeführten und eingesetzten Anwendung.** Letzten Endes bringt jede dieser Anwendungen ihre ganz eigenen Risiken für die Unternehmensumgebung mit sich, sei es nun fehlerhafter Code, exponierte APIs oder löchrige Cloud-Verbindungen, welche Kundendaten offenlegen.

Die Welt während der globalen Pandemie wurde durch mobile Verbindungen getragen, wodurch viele Unternehmen über Wasser halten konnten. Von globalen Unternehmen, deren Mitarbeiter über private Geräte auf Unternehmensdaten zugriffen bis hin zu kleinen Restaurants, die sich auf Speisekarten-QR-Codes, Online-Bestellungen und kontaktlose Zahlungen verließen – mobile Konnektivität machte es der Welt möglich, auch in einer Zeit der notwendigen Isolation in Kontakt zu bleiben. Diese Tür wurde geöffnet und wird sich auch nicht mehr schließen lassen. Mitarbeiter, Kunden, Wähler, Nutzer und Unternehmen werden auch in den kommenden Jahrzenten dieses Level der mobilen Konnektivität erwarten. Es ist an der Zeit, einen guten Kurs bei der effektiven Sicherung dieser Verbindungen einzuschlagen, um sie weiterhin zur Verfügung stellen zu können.

Wie Sie den diesjährigen Bericht am besten nutzen

Aus all diesen Gründen und in diesem Moment in der Geschichte wollen wir Ihnen einen besseren Einblick in die Rolle mobiler Bedrohungen für Geräte und Anwendungen in der allgemeinen Cybersicherheit-Bedrohungslandschaft geben.

Das Ziel unseres Berichts zu globalen Mobilbedrohungen von 2022 ist es, Einblicke zu sammeln, zu organisieren und aufzubereiten, um es weltweit agierenden Unternehmen und Organisationen zu ermöglichen, gut informierte Entscheidungen bei der Sicherung ihrer Daten zu treffen. Wir haben unsere Daten mit Blick darauf gesammelt, möglichst viele Perspektiven einzufangen, einschließlich solcher außerhalb unseres Unternehmens, um die mobile Bedrohungslandschaft aus allen Winkeln betrachten zu können.

- **Als erstes schauen wir in diesem Bericht auf die mobile Angriffsfläche und untersichen die mobilen Bedrohungsdaten eines ganzen Jahres, einschließlich eines genaueren Blicks insbesondere auf die Bedrohung von Mobilgeräten und mobilen Anwendungen.**
- **Desweiteren erkunden wir, welchen Einfluss mobile Bedrohungen und eine moderne mobile Sicherheitsstrategie auf das komplette Sicherheitsökosystem haben, mit Beiträgen unserer Partner SentinelOne, Ping Identity und Intertrust.**
- **Zuletzt erhalten Sie von uns eine Zusammenfassung und eine thematische Zusammenfassung mobiler Bedrohungsdaten im täglichen Geschehen, einschließlich bekannter mobiler Angriffsvektoren, regionalen Analysen, ausgenutzten mobilen Verwundbarkeiten, mobile Phishing-Trends sowie mobile Malware-Trends.**

Wir hoffen, dass diese Informationen und Perspektiven die Sicherheitsstrategie und Investitionen Ihrer Organisation im kommenden Jahr unterstützt, während wir alle dazu beitragen, eine sicherere und stärker verbundene Welt zu erschaffen.

Mobile Sicherheit im Einklang mit der breiteren Unternehmenssicherheitsstrategie

Jon Paterson, CTO, Zimperium

Im Verlauf der letzten Jahre haben die Sicherheitswerkzeuge um XDR und SOAR sich an die Spitze der allgemeinen Entwicklung traditioneller Sicherheitsmaßnahmen gegen immer fortschrittlichere Bedrohungen gekämpft. Identitäts- und Zugangsverwaltungswerkzeuge wurden weiterentwickelt, um skalierbare Remotezuänge zu ermöglichen und **36 % aller von uns befragten Unternehmen priorisieren Investitionen in „Zero Trust"-Architekturen im Verlauf des nächsten Jahres.**[3] Diese fortschrittlichen Sicherheitsschichten ermöglichen es Firmen, auch außerhalb der Mauern des Unternehmens effizient zu skalieren, lassen sich in bereits vorhandene Workflows zur Identitätsverwaltung integrieren und etablieren einen Schutzwall um die Geräte und Anwendungen, welche sich über die verschiedensten Netzwerke verbinden.

Doch all diese Sicherheitsinvestitionen zerbröckeln ohne den Einschluss von Mobilgeräten. Angefangen beim modernen Schutz mobiler Endgeräte und der Gerätebeglaubigung über die Sicherung von Unternehmensanwendungen bis hin zum kompletten Entwicklungszyklus benötigen Firmen Sicherheitsmaßnahmen, welche mit den vorhandenen Daten, Zugängen, Mitarbeitern und Kunden skalieren.

Die Einbeziehung moderner und mobiler Endgeräte- und Anwendungssicherheit in die Unternehmensstrategie ist nicht der Weisheit letzter Schluss, sondern lediglich der Anfang dessen, was nötig ist.

Die Integration von Geräten in unseren Alltag bereitet den Weg für die Annäherung des modernen Endgerätes. Apple hat bereits begonnen, OSX- und iOS-Dienste auf ihren Plattformen zu integrieren und Windows 11 ermöglich schon bald die native Ausführung von Androidanwendungen auf dem Desktop. Googles ChomeOS-Projekt lässt die Grenze zwischen mobilen und Desktop-Endgeräten noch weiter verschwimmen dank geteilter Anwendungen, Erweiterungen und Dienste.

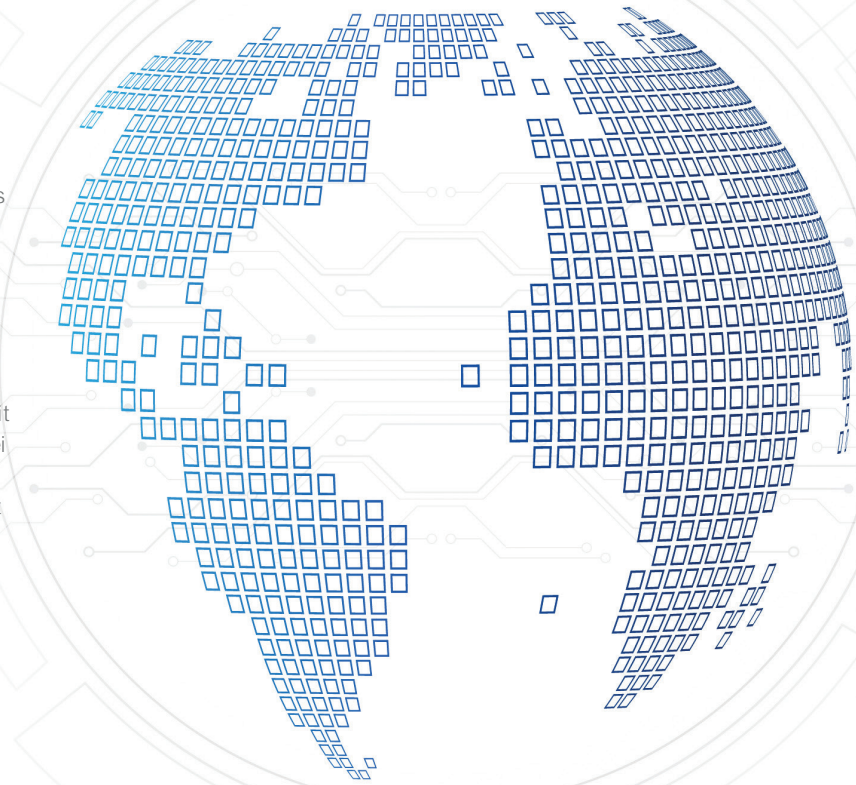
Wenn wir Anwendungen für moderne Endgeräte entwickeln, beginnt der Aufbau einer sicheren und konformen Anwendung mit der Wahl der richtigen Architektur und des richtigen Frameworks für Geräte und Plattformen, welche die Bedürfnisse Ihres Unternehmens erfüllen. Ein gutes Sicherheitsdesign ermögt gute fundamentale Entscheidungen über den Code, Daten und kryptographischen Schlüsselschutz. Sicherheitsmaßnahmen müssen Hardware- und Software-Fragmentierung berücksichtigen. **Als die Verwahrer von Daten müssen Unternehmen immer davon ausgehen, dass Anwendungen grundsätzlich in einer feindlichen Umgebung arbeiten, wodurch die Sichtbarkeit von Runtimes und der Schutz von Daten im Ruhemodus, bei der Nutzung und der Übertragung zur Priorität wird.**

Unternehmen, die sich bei der Etablierung von „Zero Trust“-Architekturen und der Anwedung von guten Sicherheitsmaßnahmen bei der Entwicklung von Anwendungen an die Spitze stellen, sind bereits für die kommende Evolution moderner Endgeräte. Bedrohungen und Risiken werden dazu in der Lage sein, genau wie legitime Daten zwischen Geräten sowie Diensten zu wechseln und Schwachstellen zu kritischen Systemen werden geteilt. Noch im September 2021 wurde das erste Auftauchen einer einzelnen Schwachstelle, welche gleich mehrere Geräte betrifft (CVE-2021-30860) gemeldet als Teil des Pegasus-Spywareangriffs, was sich auf iMessages auf iOS- und OSX-Geräten auswirkte.

Und das ist bloß der Anfang. Die Grenze zwischen mobilen und traditionellen Endgeräten wird weiter verschwimmen und damit ist es zwingend notwendig, dass die notwendigen Sicherheitsmaßnahmen bereits vorhanden und dazu bereit sind, modernen Endgeräten Sichtbarkeit, notwendige Berechtigungen und sicheren Zugang zu Unternehmen zu bieten.

Multi-Experience-Plattformen werden auch weiterhin großen Einfluss auf das Design und den Aufbau von Anwendungen haben, werden jedoch auch exponentiell den Bedarf an umfassenden und integrierten Sicherheitsplattformen erhöhen.

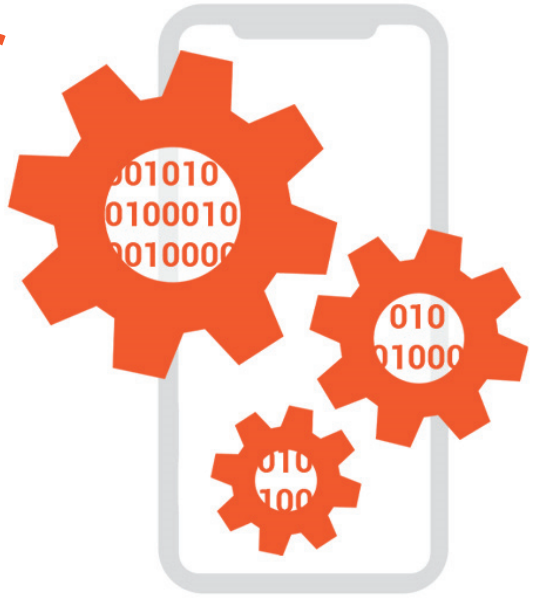
Auch die Angriffsfläche von Unternehmen wird sich weiterhin verändern und weiterentwickeln, angetrieben durch die Herausforderungen und Gelegenheiten, welche diese wachsenden Angriffsflächen bieten. Staatlich geförderte Technologien, die Ausnutzung von Schwachstellen in Anwendungen und kommerziell verfügbare Bedrohungen – das Geschäft der Cyberkriminalität wächst von Jahr zu Jahr und zeigt keine Anzeichen, sich zu verringern. Die **Auswirkungen auf Unternehmen sind auch aufgrund der im Jahr 2021 von 3,86 $ Millionen auf 4,24 $ Millionen gestiegenen Kosten für Datenlecks nicht zu übersehen.**[4]



Für mehr als ein Jahrzehnt haben wir die Grenzen der Sicherheit für mobile Endgeräte und Anwendungen ausgetestet und dabei mit fortschrittlich denkenden Partnern zusammengearbeitet, um den Risiken und Bedrohungen für die moderne Belegschaft eines Unternehmens einen Schritt voraus zu sein. Keiner von uns hätte den Einfluss der letzten drei Jahre auf globale Unternehmen vorhersehen können, doch Zimperium war bereit, mit den mobilen Bedarfen von Unternehmen weltweit zu wachsen.

Unabhängig davon, ob Sie lediglich die Risiken verstehen wollen, die mobile Endgeräte für Ihr Unternehmen mit sich bringen können oder ob Sie Bedrohungen für Ihre intern entwickelten Mobilanwendungen erkunden wollen – ich hoffe, dass unser Bericht zu globalen Mobilbedrohungen 2022 Ihnen die Daten und Ergebnisse einbringt, die Sie für eine zuversichtliche mobile Sicherheitsstrategie benötigen.

Die fortgeführte Rolle für KI und Maschinenlernen in der mobilen Sicherheit



Esteban Pellegrino, Chief Scientist, Zimperium

Ende 2019 begann in einigen wissentschaftsfokussierten Nachrichtenseiten eine unglaubliche Geschichte ihre Kreise zu ziehen, die sich hauptsächlich darum drehte, die Rechenleistung eines iPhones mit den Computern zu vergleichen, welche die NASA auf den Mond gebracht hat. Es war eine aufregende Erkundungsreise in die Geschichte der Rechenleistung einer der größten Errungenschaften der Menschheit vor 50 Jahren und wie sie mit dem kleinen Gerät zusammenhängt, dass wir jeden Tag in die Hosentasche stecken. Ohne allzu mathematisch zu werden, **kann man mit Sicherheit sagen, dass Apples iPhone 11 aus dem Jahr 2019 mehr als dazu in der Lage gewesen wäre, die Daten aller sechs Mondlandungen gemeinsam zu verarbeiten und die Landungen zu steuern. Und es hätte noch Rechenleistung übrig.**

Die Fähigkeiten dieser Mobilgeräte werden von Nutzern heutzutage als gegeben hingenommen, während man auf einen kleinen Bildschirm sieht, der dauerhaft mit einem Netzwerk verbunden ist, browsend, erkundend, navigierend und berechenend. Gelegentlich benutzt man sie sogar für einen Anruf. Doch die iPhone- und Android-Geräte, welche den Mobilmarkt heutzutage dominieren, sind mehr Computer als Telefon – permanent mit kritischen Datensystemen verbunden, voller privater Informationen und täglich im Gebrauch für das Arbeits- und Privatleben.

Vor 15 Jahren wurde das erste iPhone vorgestellt und wir durften beobachten, wie das Smartphone seinen Weg in die Unternehmen fand, ob nun verwaltet oder nicht verwaltet. Diese Computer für die Hosentasche entwickelten sich von Konsumentenaccessoires zu richtigen Geschäftswerkzeugen, mit denen Arbeitnehmer auch außerhalb des Büros mit dem Unternehmen verbunden waren. Zugänge waren anfangs noch sehr rudimentär, doch im Laufe der Jahre wurden Mobilgeräte von einem technischen Accessoirce zu kritischen Zugangsgeräte n für Dienste, Daten und Identitätsnachweise, gleichwertig in ihrer Bedeutung zum bereitgestellten Laptop. Doch im Gegensatz zu Laptops fehlten mobilen Endgeräten und den darauf verwendeten Anwendungen leider die fortschrittlichen Sicherheitsfunktionen, um bei aktuellen Bedrohungen auf dem Laufenden zu bleiben.

Vor 10 Jahren erkannte das Gründerteam von Zimperium diesen Mangel an fortschrittlichen mobilen Sicherheitswerkzeugen, um Daten und Zugänge zu sichern. **Uns war klar, dass wir diese außerhalb menschlicher Fähigkeiten liegenden Bedrohungen verstehen mussten, um Muster zu erkennen, die selbst für Experten unsichtbar waren und, noch wichtiger, dass wir nie aufhören durften, von der sich stetig weiterentwickelnden Mobilerfahrung zu lernen.**

Im Jahr 2012 erfanden und patentierten wir[5 6] Zimperium z9, das dynamische und aktualisierbare Framework für maschinelles Lernen, welches Zimperium durch die Bereitstellung von künstlicher Intelligenz direkt auf dem Gerät zum ersten Anbieter von Schutzmaßnahmen vor mobilen Bedrohungen (MTD, Mobile Threat Defense) machte.

In den letzten zehn Jahren haben wir kontinuierlich weltweit die fortschrittlichsten Sichheitsmaßnahmen an Endgeräte und Anwendungen geliefert und bleiben dadurch den wachsenden Bedrohungen des Mobilmarktes einen Schritt voraus. **Unsere Mission ist es, die Sicherheit von Anwendungen und Endgeräten über eine einzige Technologie zu vereinen und somit die Angriffsflächen von Mobilgeräten sowie den darauf installierten Anwendungen zu verringern.** Wir zielen darauf ab, mobilen Endgeräten und Anwendungen während der Entwicklung sowie der Laufzeit den fortschrittlichsten, auf die Bedürfnisse von Unternehmen abgestimmten Zero-Day-Schutz direkt auf dem Gerät anzubieten.

Heute bietet unsere fortschrittliche KI Schutz vor Malware, Netzwerkspionage und Abfangangriffen, Phishing, Hooking, Manipulation, Debugging und Ausnutzen von Schwachstellen für Mobilgeräte und Anwendungen direkt auf dem Gerät. Endgeräte und Anwendungen nutzen unsere KI-Technologie, um bereit zu sein, wenn neue Bedrohungen auftauchen und unsere Erfahrung wird auch in Zukunft den nötigen Schutz bieten, um Bedrohungen einen Schritt voraus zu sein.

Mobile und traditionelle Geräte werden immer mehr zu einem Gerät und die mobilen Versionen ersetzen immer weiter ihre traditionellen Gegenstücke in ihrer Möglichkeit, auch außerhalb des Büros auf große Datenmengen zuzugreifen und diese zu verarbeiten. Mit jedem weiteren technologischen Fortschritt einer neuen Anwendung tauchen neue Risiken und Bedrohungen auf, die Überwunden werden müssen. Es ist an der Zeit, diesen Bedrohungen direkt ins Auge zu blicken, die Zuversicht in mobilen Schutz zu erhöhen und für alles Kommende bereit zu sein.

Eines Tages werden unsere Mobilgeräte es bis zum Mond und noch viel weiter schaffen – von Wandanschlüssen getrennte Kommunikationsgeräte, die zukünftige Forscher mehr denn je mit einander verbinden. So wie die Apollo-Wissenschaftler die Rechenleistung heutiger Geräte nicht hätten voraussehen können, so wissen wir nicht, wie neue Entwicklungen in der Technologie aussehen werden. Doch wir können zuversichtlich sein, dass Mobilgeräte gekommen sind, um zu bleiben.

Umgang mit mobilen Risiken im Jahr 2022

Vorwort von Malcolm Harkins, Chief Security & Trust Officer, Epiphany Systems

> **„Risiken umgeben und umhüllen uns. Wenn wir sie nicht verstehen, riskieren wir alles und wenn wir sie nicht nutzen, bekommen wir nichts.“**

Dieses Zitat von Glynis M. Breakwell aus Ihrem Buch *„The Psychology of Risk“* sagt schon alles. Ich habe bereits seit Jahrzehnten mobiles Computing gesehen, erfahren und beworben, schon in der Zeit, als ich noch bei Intel Chief Security & Privacy Officer war.

Als der erste wirklich mobile Laptop mit allgegenwärtiger kabelloser Konnektivität (Centrino platform) im März 2003 veröffentlicht wurde, haben mein Team und ich ihn ermöglicht. Als das iPhone im Jahr 2007 veröffentlicht wurde, haben wir es ebenfalls ermöglicht – und damit über Nacht 50.000 BYOD-Geräte erschaffen. Als verschiedene Unternehmensanwendungen mobil wurden, haben wir auch diese ermöglicht. In den Jahren seit dieser frühen Mobilität gab es eine fortschreitende Explosion an Geräten und Anwendungen, die neue Gelegenheiten für ökonomisches Wachstum sowie soziale Vorteile mit sich gebracht haben, welche einen massiven positiven Einfluss auf Unternehmen und Kunden hatten.

Doch haben wir die in Kauf genommenen Risiken und ihre potentiellen Auswirkungen wirklich verstanden? In einigen Organisationen ist die Antwort ein klares „Ja“, doch in vielen leider noch immer ein „Nein“.

Zum Beispiel stellt ein im Bericht erwähnter Trend fest, dass viele iPhones und Mobilgeräte in ihrem Ökosystem genehmigt haben. War dies ein kalkuliertes Risiko, dass man in Kauf nehmen konnte, auch wenn für diese Datenzugriffskanäle noch keine Sicherheitsmaßnahmen etabliert waren? Oder hat die Verfolgung potentieller Vorteile zu einer Voreingenommenheit geführt, die nicht nur die realen Risiken für das Unternehmen unterdrückt hat sondern auch zu einem nicht unerheblichen Risiko für die Individuen geführt hat, deren persönlichen und finanziellen Daten nun gefährdet sind.

Zimperium hat den bisher umfassendsten Bericht zu mobilen Bedrohungen zusammengestellt. Er beinhaltet eine breite Sicht auf Bedrohungs- und Schwachstellentrends sowie einen Ausblick auf die Konsequenzen, welche diese auf die Sicherheit von Organisationen haben könnten. Der globale Risikobericht des Weltwirtschaftsfoums von 2022 besagt, dass „wachsende Cyberbedrohungen die Fähigkeit der Gesellschaft, diese zu verhindern und zu bewältigen, überholen“. Die Angriffsflächen wachsen weiter und ändern sich stetig, während sich die Datenverarbeitung weiterentwickelt, doch das Verstehen der Angriffstiefe im Kontext der Infrastruktur Ihres Unternehmens ist der Schlüssel zum Verständnis dessen, wie Mobilanwendungen und -geräte zu einer materiellen Exponierung führen können, welche Auswirkungen auf Ihr Unternehmen haben können.

In diesem Bericht teilt das fortschrittliche Bedrohungsforschungsteam von Zimperium zLabs tiefgreifende Details, die umfassende Einsichten für Sicherheitsteams zum Verständnis des mobilen Bedrohungslandschaft mit sich bringen. Einer dieser Trends, der die im Bericht dargestellte Landschaft von Grund auf verändern wird, ist die Annäherung von Systemen und das verschwimmen von mobilen und Desktop-Anwendungen auf modernen Betriebssystemen. Dieser Trend im speziellen wird uns „umgeben und umhüllen“ und ohne die Implementierung geeigneter Maßnahmen werden wir „alles riskieren“.

Ein weiteres von mir geliebtes Zitat ist von Art Turock:

> **„Es gibt einen Unterschied zwischen Interesse und Hingabe. Wenn Sie an etwas interessiert sind, machen Sie es, wenn die Umstände es erlauben. Wenn Sie jedoch mit Hingabe an etwas arbeiten, akzeptieren Sie keine Ausflüchte sondern lediglich Ergebnisse.“**

In Anbetracht der Trends ist es offensichtlich, dass wir gemeinsam die mobilen Risiken und die durch sie verursachten Expositionen unterschätzt haben. Ich habe schon vor vielen Jahren gelernt, dass es zwei Arten von Fehlern gibt. Die, mit denen man leben muss und die, die man beheben kann. In der letzteren Position schätzte ich mich glücklich und habe den Fehler berichtigt. All unsere Sicherheitsinvestitionen bröckeln ohne den Einschluss von mobilen Endgeräten und Anwendungen. Wir können die vergangenen Fehler in puncto Mobilsicherheit beheben und uns besser positionieren, um risikoreiche Fehler in Zukunft zu vermeiden.

Die Wahl liegt bei Ihnen und der richtige Zeitpunkt ist jetzt. Wenn Sie nicht die Entscheidung treffen, diese Risiken direkt anzugehen, sollte dieser Bericht klar darlegen, dass die Entscheidung für Sie getroffen werden wird.

Aufarbeitung mobiler Bedrohungen im Jahr 2021

42 %

Reported mobile devices & web applications led to security incident

42 %

Reported unauthorized apps & resources accessing enterprise data

10 %

Reported unsecured applications due to lack of authentication or encryption

56 %

Rely on at least four to eight enterprise applications on their mobile device

17 %

Depend on more than eight work-specific apps on their mobile device

Mobilgeräte sind nicht nur Gerät zur persönlichen Kommunikation – heutzutage sind sie ein integraler Bestandteil der Arbeitsprozesse in Unternehmen. Dank der gesteigerten Möglichkeiten und Konnektivität können Smartphones und Tablets nun auf die gleichen Daten und Dienste zugreifen wie traditionelle Geräte, ebenso wie auf eine Vielzahl neuer cloudbasierter Unternehmensdienste. Um sowohl die Produktivität von Remote-Mitarbeitern als auch die Sicherheit von Unternehmenseigentum zu stärken, müssen mobile Endgeräte proaktiv und intelligent geschützt werden.

Auch wenn traditionelle Endgeräte weiterhin genutzt werden, stehen Sicherheitsteams vor der Herausforderung, für die nötige Sichtbarkeit der Nutzung und Aktivität von Mobilgeräten zu sorgen. Diese fehlende Sichtbarkeit macht es schwer und zeitaufwendig für Teams, Bedrohungen aufzuspüren und entsprechende Maßnahmen zu ergreifen. Außerdem erweitert sich mit jedem weiteren Endgerät, das auf Unternehmenssysteme zugreift, die Angriffsfläche und damit das Risiko schädlicher Aktivitäten.

In einer kürzlichen Umfrage wurden führende Persönlichkeiten in der Technologie darum gebeten, fünf Bedrohungen hervorzuheben, welche in den vorhergehenden zwölf Monaten die größten Auswirkungen auf ihre Systeme hatten. **42 % der Befragten teilten mit, dass Mobilgeräte und Webanwendungen zu einem Sicherheitsvorfall geführt haben.** Doch nicht nur mobile Endgeräte bringen Risiken für Unternehmenssysteme mit sich: Weitere 42 % der Befragten berichteten von unautorisierten Apps und Ressourcen, die auf Unternehmensdaten zugriffen und 10 % meldeten ungesicherte Anwendungen aufgrund von fehlender Authentifizierung oder Verschlüsselung.[7]

Es ist nun wichtiger und herausfordernder als je zuvor, eine Balance zwischen dem Zugang für Mobilgeräte und der Angriffsflächenminimierung für Unternehmen zu finden. Ob Firmen nun vom Unternehmen besessene und verwaltete Endgeräte verwenden oder ein aktives Bring-your-own-device-Programm haben – mobile Endgeräte und Anwendungen sorgen für gesteigerte Risiken. 56 % der befragten Personen verlassen sich für ihren Arbeitsfluss auf mindestens vier bis acht Unternehmensanwendungen. **17 % der befragten Personen verlassen sich auf mehr als acht arbeitsspezifische Anwendungen auf ihren Mobilgeräten.**[8] Auch wenn diese Anwendungen zwischen Drittanbieteranwendungen und intern entwickelten Werkzeugen variieren, verlassen sich beide Kategorien auf den Zugang zu unternehmensinternen Systemen, um effizient zu funktionieren.

Angriffe auf Mobilgeräte und Anwendungen hatten negative Auswirkungen auf Systeme, die Privatsphäre, Kundendaten und mehr. Aufgrund des Zugriffs auf und der Verarbeitung von kritischen Informationen mit diesen Geräten, wie Passwörterm, Multifaktor-Authentifizierungsanwendungen, Unternehmensdaten und -Kommunikation, ist es keine Überraschung, dass sich die Bedrohungen in den letzten Jahren vermehrt haben und dass arglistige Akteure weiterhin darin investieren, diese Geräte und Anwendungen mit immer komplexeren Methoden ins Visier zu nehmen.

Vor der COVID-19-Pandemie hatten 60 % der Organisationen keine aktiven BYOD-Regelungen.[9] Im Verlauf der letzten zwei Jahre haben viele Teams heroisch und blitzschnell reagiert, um ein Arbeiten außerhalb des Büros zu ermöglichen. Doch die daraus folgende Steigerung der vorhandenen BYOD-Regelungen verwischt weiterhin die Grenzen zwischen Geräten und Daten sowie zwischen Verbracuherbedrohungen und Unternehmensbedrohungen. Desweiteren ist es wichtig zu verstehen, dass Arbeitnehmer genauso wie Verbraucher ihre Privatsphäre schützen wollen. Unter anderem sind es Vertrauens- und Privatsphärebedenken unter Arbeitnehmern, welche die Adaption von Geräteverwaltungsrichtlinien in Unternehmen verlangsamen.

Bei unserer Beurteilung der mobilen Bedrohungslandschaft war das Jahr 2021 das Jahr der großen Offenbarungen und Neuentdeckungen von bereits bekannter Malware. Pegasus, das Spyware-Program, welches Regierungen weltweit verkauft wurde, tauchte erneut in den Nachrichten auf, nachdem eine Kampagne aufgedeckt wurde, die 50.000 Journalisten, Menschenrechtsaktivisten, politische Führungspersönlichkeiten und mehr als Ziel hatte. Die initial von Amnesty International aufgedeckte Kampagne bestand unter anderem aus Zero-Day-Exploits, die iOS-Geräte zum Ziel hatten. Die Schockwellen dieser Entdeckung waren noch Monate später zu spüren, während immer neue Informationen über die Angriffe und deren Opfer ans Tageslicht kamen.

Der erstmals 2017 entdeckte Trojaner „Joker“ tauchte erneut im Jahr 2021 erneut auf, diesmal dank erweiterter Möglichkeiten mit Android-Geräten als Ziel. Diese Trojaner sind bösartige Android-Anwendungen, bekannt dafür, Rechnungsbetrug zu begehen und für Nutzer Abonnements zu Premiumdiensten abzuschließen. Wie bei vorherigen Formen dieser Angriffe hatten auch die neu entdeckten Trojaner das gleiche Ziel: finanzielle Vorteile. Die erfolgreiche Infektion von Mobilgeräten erfolgt häufig, ohne dass das Opfer etwas davon merkt, bevor der Schaden angerichtet und das Geld verschwunden ist, wodurch die Betroffenen in der Regel keine Möglichkeit haben, den Angriff zu unterbinden.

Mitte 2021 wurden mehr als 1.000 Versionen der Joker-Malware entdeckt, doch diese neuen Varianten verfügten in ihrem Code über neue Methoden, um Sicherheitsmaßnahmen zu umgehen.

Die Ausnutzung von Geräteschwachstellen, falsch konfigurierte Anwendungen, Malware und undichte Datenbanken: Mobilgeräte sind ein längst reifes Ziel für bösartige Akteure weltweit. Zimperiums Daten aus dem Jahr 2021 zeigen, dass es keinen Mangel an Bedrohungen spezifisch für mobile Ökosysteme gibt. Doch dank der gelernten Lektionen des letzten Jahres sollte 2022 das Jahr sein, in dem die Menschen beginnen, Mobilgeräte und -Anwendungen mit der gleichen fortschrittlichen Einstellung zum Thema Sicherheit zu betrachten wie es bei traditionellen Endgeräten bereits der Fall ist.

2022 Zimperium zLabs Forschungs-Highlights

Zimperiums fortschrittliche zLabs Forschungsgruppe untersucht fortlaufend Mobilgeräte- und Anwendungsbedrohungen, die Nutzer weltweit zum Ziel haben. Im Vergleich zu vorangegangenen Jahren gab es im Jahr 2021 eine Steigerung der verfügbaren Daten und Medienberichte zu Mobilbedrohungen und es gab einen größeren Fokus auf iOS- und Android-Angriffsvektoren. **Während des Jahres 2021 hat Zimperiums zLabs-Team eine Vielzahl an Bedrohungen entdeckt, welche Auswirkungen auf mehr als 10 Millionen Geräte in mindestens 214 Ländern hatten.**

Hier ist eine Zusammenfassung der bemerkenswertesten Entdeckungen durch Zimperiums zLabs Bedrohungserforschungsteam:

Forensische Nachweise dieses aktiven Trojanerangriffs auf Androidgeräte, welchen wir **GriftHorse** genannt haben, legen nahe, dass diese Bedrohungsgruppe bereits seit November 2020 aktiv ist. Diese böswartigen Anwendungen wurden initial sowohl durch Google Play als auch über Appstores von Drittanbietern verteilt. Diese Kampagne hatte Mobilgerätenutzer aus mehr als 70 Ländern zum Ziel. GriftHorse ist extrem flexibel. Die angezeigten Inhalte sowie die verwendete Sprache konnten basierend auf der IP-Adresse des Nutzers angepasst werden. Zwischen November 2020 und September 2021 (als die Schadsoftware öffentlich aufgedeckt wurde) hatte GriftHorse es geschafft, mehr als 10 Millionen Geräte zu infizieren. Nach einer Meldung durch das Zimperium zLabs-Team entfernte Google die bösartigen Anwendungen aus seinem Store.

Bisher hat das Zimperium zLabs-Team insgesamt 23 Anwendungen aufdeckt, welche Bürger Südkoreas zum Ziel hatten. Diese Spyware infizierte die Geräte von tausenden ahnungslosen Nutzern. Die bösartigen Android-Apps wurden entwickelt, um ihr kontinuierlich auszuspionieren. Sie laufen heimlich und unentdeckt im Hintergrund und erregen in der Regel keine Aufmerksamkeit. Wir haben Grund zu der Annahme, dass die für **PhoneSpy** verantwortlichen Personen eine erhebliche Menge an persönlichen und Unternehmensdaten von ihren Opfern gesammelt haben, einschließlich privater Kommunikation und Fotos. Nach der Offenlegung wurde diese spezifische Spyware-Kampagne deaktiviert und der Kommando- und Kontrollserver wurde abgeschaltet. Infizierte Geräte stehen nicht länger unter der Kontrolle der Angreifer.

Forensische Untersuchungen dieses aktiven Android-Trojanerangriffs, von uns **FlyTrap** benannt, weisen auf kriminelle Gruppen hin, die aus Vietnam heraus operieren. Diese Übernahmeangriffe geschehen seit März 2021. Diese böswartigen Anwendungen wurden initial sowohl durch Google Play als auch über Appstores von Drittanbietern verteilt. Die für diese Bedrohung Verantwortlichen nutzen die Tatsache für sich aus, dass Nutzer häufig der fehlerhaften Annahme anhängen, dass ein Login in die richtige Domäne immer sicher ist, unabhängig von der genutzten Anwendung. Bei den ins Visier genommenen Domänen handelte es sich um beliebte Social Media Plattformen, wobei diese Kampagne ausgesprochen effektiv dabei war, die Sitzungsdaten in sozialen Medien in mehr als 144 Ländern abzugreifen. Diese kompromittierten Accounts können als Botnetz für verschiedene Zwecke verwendet werden. Zum Beispiel ist es den Akteuren so möglich, die Beliebtheit bestimmter Seiten oder Produkte künstlich zu steigern. Zusätzlich können diese Account genutzt werden, um Falschinformationen und politische Propaganda zu verteilen. Google hat nach der Meldung durch Zimperiums zLabs-Team die bösartigen Anwendungen entfernt.

Die „System Update“-App wurde von Zimperiums zLabs-Team mithilfe der z9 Malware-Engine identifiziert, welche Grundlage der zIPS-Bedrohungsermittlung direkt auf Geräten ist. Nach einer Untersuchung stellten Forscher fest, dass es sich hierbei um komplexe Spyware mit vielen Möglichkeiten handelt. Die Mobilanwendung stellt eine Bedrohung für Androidgeräte dar, indem sie als Fernzugriffstrojaner (RAT, „Remote Access Trojan“) fungiert. Die Anwendung erhält Anweisungen zum Sammeln und Abgreifen einer Vielzahl an Daten und zur Ausführung einer breitgefächerten Reihe von bösartigen Aktionen. Sobald die Kontrolle übernommen wurde, können die Hacker Audio und Telefonanrufe aufzeichnen, Fotos machen, den Browserverlauf einsehen, auf WhatsApp-Nachrichten zugreifen und vieles mehr.

Dank der Analyse durch Zimperiums zLabs-Team konnte festgestellt werden, dass 14 % der iOS- und Android-Anwendungen, welche weltweit verfügbar waren, mehrere massive Fehlkonfigurationen aufwiesen. Diese Apps nutzten Cloudspeicher mit ungesicherten Konfigurationen. Diese Probleme sorgten für die Aufdeckung von persönlich identifizierbaren Informationen (PII, „Personally Identifiable Information“), ermöglichte so Betrugsversuche und deckte IP-Adressen oder interne Systeme und Konfigurationen auf. Falsch konfigurierte Anwendungen ließen sich in beinahe jeder Kategorie finden.

Das Bild unten zeigt die Verteilung von Apps mit Problemen aufgrund von ungesichertem Speicher über die verschiedenen Kategorien.

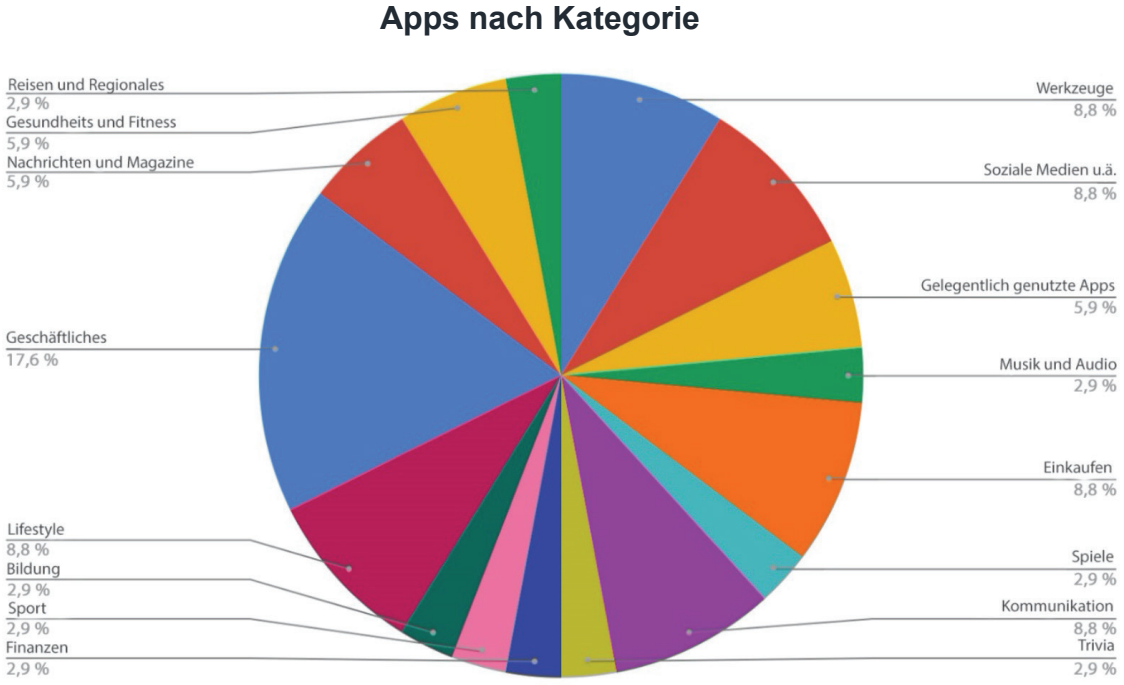


Abbildung #: Anwendungen mit ungesichertem Cloudspeicher, nach Kategorie.

Die zehn Angriffe, die Mobilbedrohungen im Jahr 2021 in die Schlagzeilen gebracht haben

Mit dem Aufstieg immer komplexerer Angriffe, Zero-Day-Schwachstellen und nennenswerten Exploits ist es keine Überraschung, dass die Medien ausgiebig zu diesen Themen berichtet haben. Laut der Cision-Medienbeobachtungsplattform wurden iOS- und Android-Sicherheitsnachrichten weltweit von einer Vielzahl von Medienunternehmen abgedeckt.

Dies ist eine Liste der zehn am häufigsten abgedeckten Bedrohnungen und Links zu Beispielartikeln.

1 Apple iOS: iOS 14.4.2 – Schwachstelle in Apples WebKit-Browserengine

Berichterstattung: Forbes, CNET, 9to5Mac, MacObserver, MacWorld, MacRumors, Appleosophy, TechGig, Laptop Mag

2 Android: GriftHorse (Von Zimperium öffentlich gemacht)

Berichterstattung: WIRED, PC Magazine, Forbes, ZDNet, CPO Magazine, Security Week, Threatpost, Security Affairs, The Record, SensorsTechForum, HackRead, Android Headlines, Android Authority, TechTimes, iTechPost

3 Apple iOS: iOS 14.8 – Spyware-Schwachstelle (Pegasus)

Berichterstattung: Forbes, CNET, The Verge, ComputerWorld, TechRepublic, TechRadar, TechNadu, Macworld, Ubergizmo, Apple Insider, TechStory, MacRumors, PhoneScoop

4 Android: FlyTrap (Von Zimperium öffentlich gemacht)

Berichterstattung: Business Insider India, InfoSecurity Magazine, TechRepublic, PC Magazine, ZDNet, Threatpost, Bleeping Computer, Security Affairs, TechRadar, TechNadu, TechTimes, iTechPost

5 Android: Qualcomm- und Mail-GPU-Schwachstellen

Mai 2021 - CVE-2021-1905 (NIST-CVSS Punkte: 7.8)
Mai 2021 - CVE-2021-1906 (NIST-CVSS Punke: 5.5)
Mai 2021 - CVE-2021-28663 (NIST-CVSS Punke: 8.8)
Mai 2021 - CVE-2021-28664 (NIST-CVSS Mai: 8.8)

Berichterstattung: ArsTechnica, Security Week, Threatpost, Security Affairs, Bleeping Computer, The Record, IT Pro UK, TechNadu, Tom's Guide

6 Android: PhoneSpy (Von Zimperium öffentlich gemacht)

Berichterstattung: TechCrunch, ZDNet, The Hacker News, Security Week, Threatpost, Bleeping Computer, Security Affairs, TechRadar, HackRead, Android Community, Android Headlines

7 Android: SharkBot

Berichterstattung: SC Magazine, ZDNet, BankInfoSecurity, The Hacker News, Security Week, Security Affairs, The Record, TechTimes, The Digital Hacker

8 Apple iOS: 14.7 – Schwachstelle WifiDemon

Berichterstattung: The Hacker News, Bleeping Computer, Threatpost, Security Week, The Record, Help Net Security, We Live Security, Security Affairs, HackRead, Tom's Guide, iPhone Hacks

9 Android: Qualcomm-Schwachstelle

CVE-2020-11261 (NIST-CVSS Punkte: 7.8)

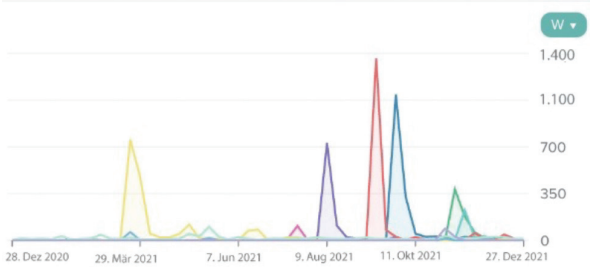
Coverage: Security Week, The Hacker News, Threatpost, Security Affairs, The Record, IT Pro UK, SensorsTechForum

10 Android: Kernelschwachstelle –

November 2021: CVE-2021-1048 (NIST-CVSS Punkte: 7.8)

Berichterstattung: Security Week, Threatpost, Security Affairs, Bleeping Computer, We Live Security, 9to5 Google, SensorsTechForum

Erwähnungen insgesamt über Zeit

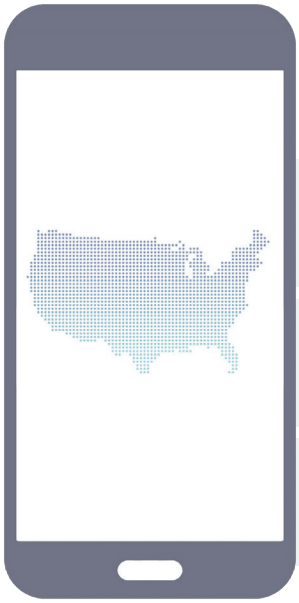


Suchname	Erwähnungen insgesamt
iOS 14.4.2	1.800
GriftHorse	1.700
iOS 14.8	1.700
FlyTrap	999
CVEs May 2021	902

Suchname	Erwähnungen insgesamt
PhoneSpy	688
SharkBot	299
WifiDemon	131
CVE-2021-1048	126
CVE-2020-11261	119

Quelle: Cision

Stand mobiler Endgerätesicherheit im Jahr 2022



Mobilgerätemarkt

Unsere Smartphones ermöglichen uns auch weiterhin, innovativ zu sein, uns zu unterhalten und eine gesteigerte Lebensqualität zu genießen. Natürlich wachsen in Anbetracht dessen die Verkäufe von Mobilgeräten weiter an. Im Jahr 2020 wurden weltweit fast 1,38 Milliarden Smartphones verkauft[10] In den Vereinigten Staaten gibt es mehr als 290 Millionen Smartphone-Nutzer. Die Verwendungsrate ist Jahr für Jahr gewachsen und hat im Jahr 2021 85 % erreicht.[11]

Anzahl der Smartphonenutzer in den Vereinigten Staaten

294,15 Millionen

Smartphonelieferungen 2021, Vereinigte Staaten

147,48 Millionen

Prognose Smartphone Verkaufsumsatz, Vereinigte Staaten 2021

73 Milliarden US-Dollar

Für den Smartphonemarkt der USA wird ein Absatz von 73 Milliarden US-Dollar prognostiziert, was eine massive Steigerung zu den 18 Milliarden US-Dollar Einnahmen im Jahr 2010 ist.[12] Auf dem US-Markt sind Apple und Samsung die führenden Smartphone-Hersteller. Zusammen decken sie 82 % der Verkäufe ab.[13] So wie der Markt für Mobilgeräte weiter wächst, werden es auch Mobilbedrohungen.

Für Sicherheitsteams ist es harte Realität, dass es nur eines braucht – ein geteiltes Passwort, ein getäuschter Mitarbeiter, nur ein kompromittiertes Gerät – um ein Unternehmen völlig zu exponieren. Im Verlauf der Pandemie und dem damit einhergehenden explosionsartigen Wachstum der Remote- und Hybridarbeit haben sich die mit Mobilgeräten zusammenhängenden Bedrohungen massiv erweitert. Beim Kampf gegen dauerhafte und sich ständig weiterentwickelnde Bedrohungen müssen Sicherheitsteams immer mehr Endgeräte und stetig expandierende Angriffsvektoren schützen.

BYOD Stats

Ungeachtet der steigenden Bedrohungen ermöglichen immer mehr Unternehmen BYOD-Regelungen. Leider scheitern viele Teams in der Eile, die Voraussetzungen für Remotearbeit zu ermöglichen, an der Implementierung robuster Sicherheitsmaßnahmen, die für den Schutz solcher Geräte notwendig sind.

In einer Umfragee haben wir festgestellt, dass 74 % der Befragten eine aktive BYOD-Regelung verwenden. In einer weiteren Umfrage antworteten 30 % der Befragten, dass BYOD-Regelungen innerhalb des Unternehmens eine der größten Endgeräte-Sicherheitsfragen darstellten.[14]

Die größten Endgeräte-Sicherheitsfragen

35 % Remotearbeit/ Nutzer

30 % BYOD

11 % Mobiltelefone/ Geräte

Time to Patch

In einer verteilten Belegschaft nuten Mitarbeiter ihr eigenes Netwerk und, in einigen Fällen, ihre persönlichen Geräte für die Arbeit. Diese Praktiken bringen für Unternehmen signifikante Risiken mit sich, erweitern die Angriffsfläche und vermindern die Möglichkeiten des Sicherheitsteams, bösartige Aktivitäten aufzudecken oder zu beheben. Während Teams versuchen, Risiken zu minimieren und nicht autorisierte Zugriffe auf sensible Unternehmensdaten zu verhindern, stellen BYOD-Regelungen und solche für Gastzugriffe laut 42 % der Befragten die größten Herausforderungen dar.[15]

Nach der Veröffentlichung eines Notfall- oder Prioritätspatches benötigen Teams in der Regel folgende Zeiträume zur Implementierung eines Hotfixes:[16]

42 % geben weniger als zwei Tage an

28 % geben drei bis sieben Tage an

20 % geben eine bis zwei Wochen an

Im Jahr 2021 gaben **50 %** der Befragten an, dass ihre Home-Office-Strategie ein signifikanter Faktor in Cybersicherheitsvorfällen war.

Mobile Endgeräte: Ein kritischer Teil der Cybersicherheitslandschaft

Wenn Unternehmen ihre mobilen Endgeräte nicht absichern, ist ihre Sicherheitsabteilung (SOC, „Security Operations Center“) nicht in der Lage, einen umfassenden Einblick in ihre Cybersicherheitslage zu erhalten. Wenn Mitarbeiter ein persönliches Mobilgerät verwenden, um eine E-Mail zu senden, auf Textnachrichten zu antworten oder auf sichere Unternehmensanwendungen zuzugreifen, kann das SOC diese Aktivitäten nicht überwachen oder potenzielle Risiken erkennen. Im Zuge der Zunahme von BYOD- und Heimarbeit-Szenarien müssen Führungskräfte ihre Sichtweise auf die Sicherheit mobiler Geräte ändern.

Fast die Hälfte der Umfrageteilnehmer (44 %) hat aufgrund von Cybersicherheitsvorfällen innerhalb der dezentralisierten Belegschaft zusätzliche Sicherheitsrichtlinien oder -anforderungen aufgestellt. Davon haben 40 % die Authentifizierungsverfahren für ihre Mitarbeiter geändert, während 34 % den Sicherheitsanbieter oder -dienstleister gewechselt haben.[17]

Microsoft Office ist ein bevorzugtes Ziel für kriminelle Akteure. **Einem Bericht zufolge entfielen mehr als 72 % der Angriffe auf Microsoft Office und 13 % auf Browser.[18]**

Diese Zahlen mögen beunruhigend erscheinen, aber fast die Hälfte der Technologieführer ist der Meinung, dass die derzeitigen Verfahren für die Reaktion auf Zero-Day-Vorfälle ausreichend sind.[19] Die Wahrheit ist jedoch, dass mobile Endgeräte ohne umfassende mobile Gefahrenabwehr weiterhin eine Art schwarzes Loch darstellen, wenn es um die Reaktion auf Vorfälle geht. 39 % dieser Führungskräfte sind sich darüber im Klaren, dass die Reaktionszeit mit ihren derzeitigen Verfahren zu langsam ist.[20]

48 %

der Unternehmen überprüfen ihre Cybersicherheitsstrategie regelmäßig und passen sie bei Bedarf an.

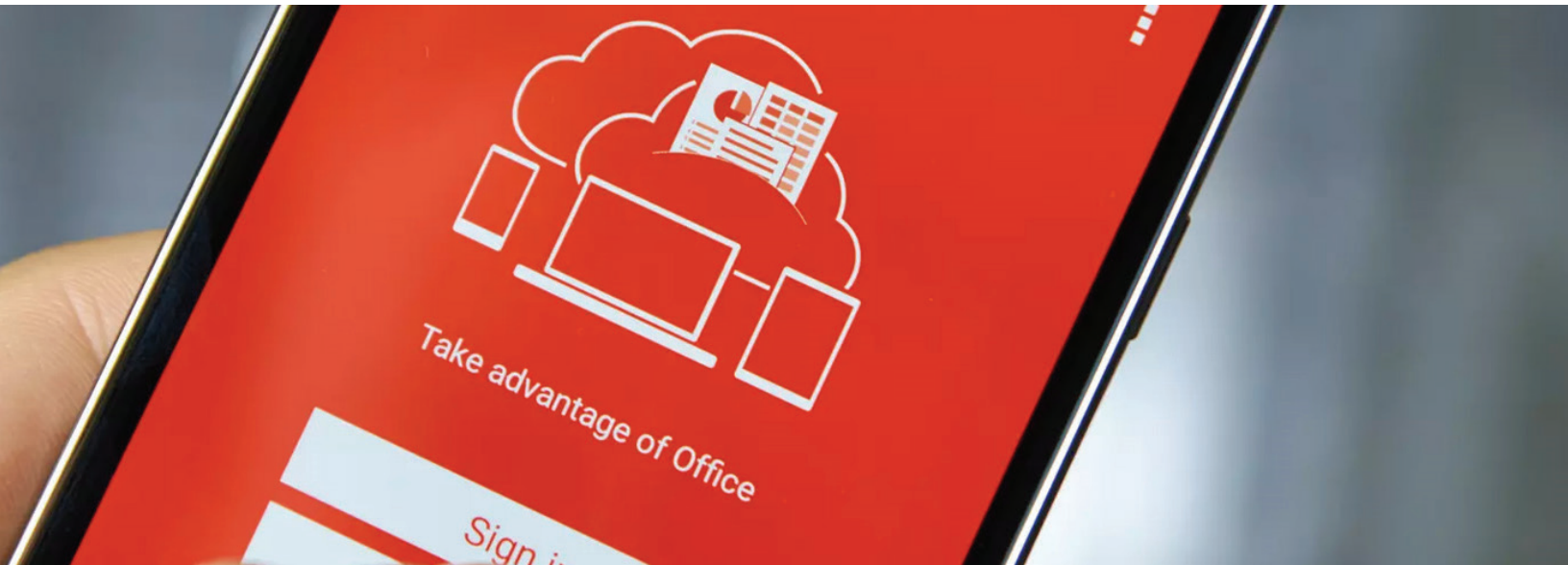
26 %

der Unternehmen entwickeln ihre Cybersicherheitsstrategie in Echtzeit oder nach Bedarf.

23 %

der Unternehmen verfügen über eine formelle Cybersicherheitsstrategie, überprüfen diese aber kaum oder verwenden überhaupt keine Sicherheitsstrategie.

Abbildung #: Die Aufschlüsselung der Cybersicherheitsstrategie von Unternehmen[21]



Mobilgeräte im Unternehmens-Ökosystem

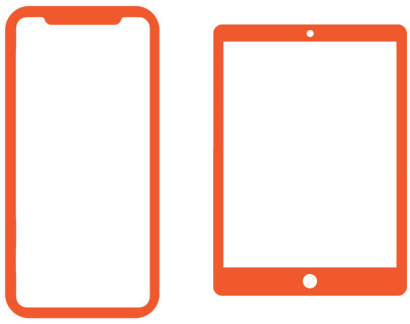
IT- und Sicherheitsteams werden weiterhin unter zunehmendem Druck stehen, da die Bedrohung durch Cyberangriffe weiter steigt, CISOs strengere Cybersicherheitsrichtlinien einführen und Mitarbeiter sich zunehmend Sorgen um den Datenschutz machen. **Mehr als die Hälfte (61 %) ist der Meinung, dass die Festlegung und Durchsetzung von Unternehmensrichtlinien im Bereich der Cybersicherheit nahezu unmöglich ist, da die Grenzen zwischen Privat- und Berufsleben stetig weiter verschwimmen.**[22] Während 46 % der Befragten der Meinung sind, dass Mobilgeräte im Unternehmensumfeld akzeptabel sind, machen sich 34 % Sorgen um den Datenschutz.[23]

66 %

der im Unternehmen genutzten Smartphones befinden sich im Besitz der Mitarbeiter.[24]

29 %

der im Unternehmen genutzten Smartphones werden vom Unternehmen selbst gekauft.



55 %

der Unternehmen genutzten Tablets befinden sich im Besitz der Mitarbeiter.[25]

39 %

der im Unternehmen genutzten Tablets werden vom Unternehmen selbst gekauft.

Abbildung #: Verteilung mobiler Geräte in Unternehmen.

Mobile Bedrohungslandschaft im Unternehmensbereich

Im Jahr 2021 analysierte Zimperium eine Reihe von mobilen Bedrohungen, einschließlich Malware, unautorisierte Zugriffe und Schwachstellen anhand der ins Visier genommenen Geräte. Erfolgreiche Angriffe auf Mobilgeräte wirken sich auf den Nettoprofit aus und kosten Unternehmen Millionen von Dollar. Zu den Konsequenzen gehören der Verlust des Kundenvertrauens, Anwaltskosten, Geldstrafen, Rufschädigung, Diebstahl sensibler Daten und vieles mehr.

Die Aufdeckung und Beseitigung von Insider-Bedrohungen ist mit den höchsten Kosten verbunden. Während unternehmenseigene Geräte und solche unter BYOD-Regelungen für den Zugriff auf Unternehmensdaten genutzt werden, haben mobile Geräte ohne Werkzeuge wie die mobile Gefahrenabwehr nur eine begrenzte Sichtbarkeit für IT-Abteilungen und es kann länger dauern, bis bösartige Aktivitäten entdeckt werden, wenn überhaupt. Laut Umfragedaten stellen Finanzabteilungen die größte interne Bedrohungsgruppe für Unternehmen dar, da diese Teams täglich sensible Finanz- und Unternehmensdaten verarbeiten.[26] Diese Statistiken unterstreichen, warum sich CEOs und CISOs auf dieses Thema konzentrieren und die Investitionen in die Endgerätesicherheit erhöhen müssen.

Im Jahr 2021 stieg das Wagniskapital für Cybersicherheit auf einen Rekordwert von 11,5 Milliarden US-Dollar. Die Umfrageteilnehmer schätzen, dass sie 43 % ihrer Mittel für die Sicherung der Cloud, 14 % für Sicherheitsberatung und 14 % für Risiko und Compliance ausgeben werden. Während der COVID-19-Pandemie erzielten Unternehmen die größte Rendite aus ihren Investitionen in die Endgerätesicherheit, gefolgt von Investitionen in die Geschäftskontinuität und die Notfallwiederherstellungsplanung.[27] Inzwischen geben 45 % der Technologieführer an, dass Mobilgeräte die größte Sicherheitslücke darstellen.[28]

Bedrohungen, die das Unternehmen in den letzten 12 Monaten betrafen[29]

54 %
Malware (Viren, Phishing, Ransomware)

46 %
Identitäts- oder Accountdiebstahl

42 %
Sicherheitslücken in Mobil- oder Webanwendungen

42 %
Unautorisierte Zugriffe auf Anwendungen oder Ressourcen

Markt für mobile Sicherheit

Die Investitionen in die Erkennung von und Reaktion auf Endgerätebedrohungen nehmen aufgrund des stetigen Anstiegs von Cyberbedrohungen für mobile Geräte immer mehr zu. Ein großer Teil dieses Wachstums wird durch mobile Zahlungen und die zunehmende Notwendigkeit, BYOD-Programme im Unternehmen abzusichern, angetrieben.

Bezogen auf die wichtigsten Regionen des globalen Sicherheitsmarktes hält Nordamerika mit 41,1 % den höchsten Anteil an Investitionen.[30] Dies könnte sich jedoch schnell ändern, da mehrere asiatische Länder, darunter China, Singapur und Japan, stark in die Entwicklung nationaler Cybersicherheitsmaßnahmen, insbesondere im Bereich der mobilen Sicherheit, investiert haben.

Mobile Gefahrenabwehr (MTD, „Mobile Threat Defense“) ist eine eigene Kategorie mobiler Sicherheitstechnologien, deren Marktanteil schnell wächst, da sie die Bedrohungserkennung und die Reaktion darauf auf mobilen Geräten verbessert. Sicherheitsexperten sind der Überzeugung, dass MTD die Mindestvoraussetzung zum Schutz vor modernen mobilen Bedrohungen ist, da die Lösung vor Angriffen auf der Geräte-, Netzwerk- und Anwendungsebene schützen kann. Darüber hinaus schützt MTD Endbenutzer vor Phishing-Angriffen, die auf Vektoren wie SMS, Messaging-Apps, persönliche E-Mails und Unternehmens-E-Mails abzielen, während Lösungen zur mobilen Geräteverwaltung (MDM, „Mobile Device Management“) über diese Funktionen nicht verfügt.

MTD geht weit über die Verwaltung von Einstellungen und Passcode-Funktionen sowie den Schutz des Netzwerks durch ein integriertes virtuelles privates Netzwerk (VPN, „Virtual Private Network“) hinaus. Die Erkennungsfunktionen warnen Administratoren vor gefährlichen Wi-Fi-Zugangspunkten, analysieren das Risiko des mobilen Ökosystems und spüren veraltete Betriebssysteme auf, sodass Teams bösartige Aktivitäten eindämmen können. Die Bedrohungsdaten der Geräte ermöglichen MTD die nötige Transparenz, um die Erkennung zu verbessern und die lateralen Bewegungen von Angreifern zu identifizieren. Auf diese Weise kann MTD Teil einer umfassenderen, einheitlichen Endgerätesicherheitsinfrastruktur (UES, „Unified Endpoint Security“) sein. MTD wird weiterhin die Führung im Bereich der mobilen Sicherheit übernehmen und ein wichtiger Bestandteil eines UES- oder erweiterten Erkennungs- und Reaktionssystems (XDR, „Extended Detection and Response System“) sein, das die allgemeine Sicherheitslage eines Unternehmens verbessert.

Stand der Sicherheit mobiler Anwendungen 2022

In einem relativ kurzen Zeitraum hat sich unsere Nutzung von Mobilgeräten und -anwendungen dramatisch verändert und erweitert. Dank der sich weiterentwickelnden Mobil- und Cloud-Technologien treiben innovative mobile Apps den digitalen Wandel in Unternehmen voran und sorgen dafür, dass unser Alltag reibungsloser verläuft.

Heutzutage ist die Reichweite des Marktes für Mobilanwendungen riesig. **Allein im Jahr 2020 wurden 218 Milliarden Mal Apps heruntergeladen.**[31] Bis 2023 wird der jährliche Umsatz mit mobilen Anwendungen voraussichtlich 935 Milliarden US-Dollar erreichen, wobei Kategorien wie Videostreaming, Spiele und Online-Fitness allesamt Milliarden von US-Dollar an Umsatz generieren.[32] Allein der Zahlungsverkehrssektor machte 2020 weltweit 1,3 Billionen US-Dollar aus.[33]

Entwicklungstrends bei Anwendungen

Im Angesicht der Profitabilität von Apps haben sich auch die Innovationen bei der Entwicklung mobiler Annwendungen stark beschleunigt. Hier sind einige der wichtigsten Trends in der Anwendungsentwicklung, welche die Landschaft der mobilen Anwendungen verändern:

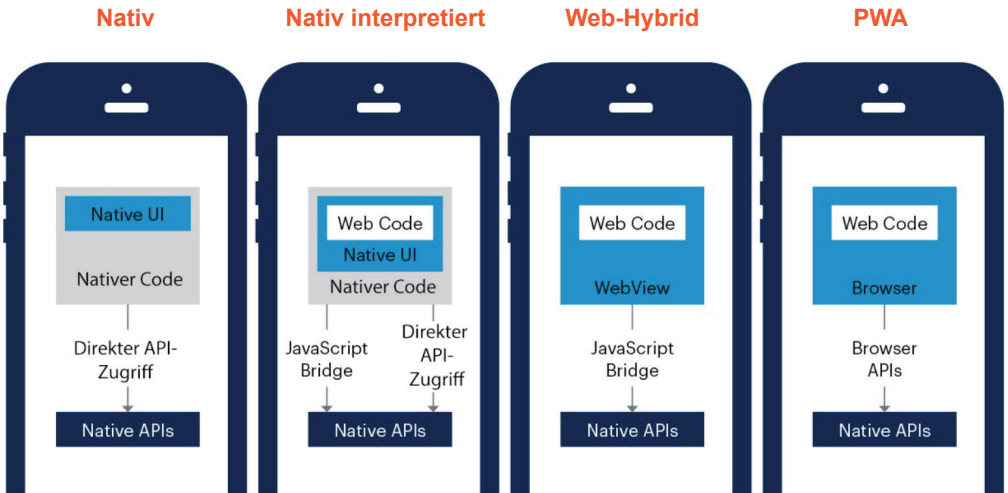
Entwicklung plattformübergreifender Mobilanwendungen

Durch hybride App-Ansätze können Entwickler mit einer einzigen Codebasis arbeiten, die sowohl auf Android- als auch auf iOS-Plattformen ausgeführt werden kann, was eine Reihe attraktiver Vorteile bietet. Entwickler können zwischen verschiedenen modernen Mobilanwendungsarchitekturen wählen. Diese Alternativen unterstützen alle Gerätearten (einschließlich Telefone und Tablets) sowie alle Plattformen (einschließlich Android und iOS). Dieser Hybrid-Ansatz bietet unschätzbare Vorteile, wenn es um Portabilität, Wartung und Verteilung geht. Es ist nicht überraschend, dass die Beliebtheit von Hybrid-Frameworks, wie zum Beispiel React, Flutter, Uno, Kotlin und Xamarin, stark gewachsen ist.

Sowohl native als auch Web-Hybridanwendungen enthalten eine Kombination nativen Codes und Webcode, wenn auch in verschiedenen Abstufungen. Bei Web-Hybridanwendungen handelt es sich weitestgehend um eigenständige Webanwendungen, die man in jedem beliebigen Browser ausführen kann. In beiden Fällen ist der Webcode jedoch aufwendiger in der Absicherung aufgrund des Mangels an Sicherheitsfunktionen in der Websteuerung und der geringeren Verfügbarkeit von Softwareentwicklungssystemen (SDK, „Software Development Kit“) und Werkzeugen für Webcode.

Progressive Webanwendungen sind eine Weiterentwicklung herkömmlicher Webanwendungen, haben aber das Aussehen und die Bedienung nativer mobiler Anwendungen. Eine einzige Codebasis unterstützt mehrere Plattformen, was die Portabilität erhöht, jedoch die Absicherung von Daten und Code erschwert.

Mobilapp-Architekturprofle



Low-Code- und No-Code-Plattformen

Die Umstellung auf No-Code- und Low-Code-Entwicklungsplattformen ist zwar schon seit einiger Zeit im Gange, aber der erhebliche Fachkräftemangel, von dem Unternehmen in den letzten Jahren betroffen waren, hat diese Umstellung dramatisch beschleunigt. In Anbetracht dieses Personalmangels wird sich die Anwendungsentwicklung zunehmend vom Schreiben von Code zu einem Zusammenstellen und Integrieren von Open-Source- und Drittanbieter-Komponenten entwickeln.

Reibungslose, immersive mobile Nutzererfahrung

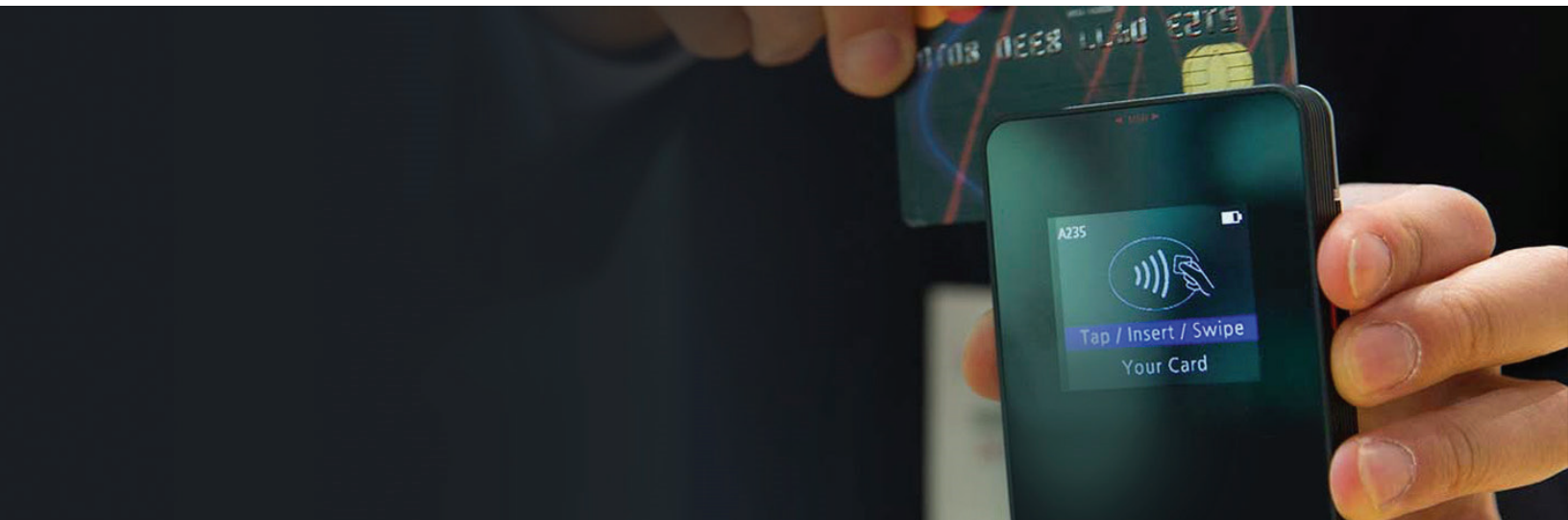
Die Fortschritte bei der passwortlosen Authentifizierung und der Sprachintegration werden die Interaktion mit unseren mobilen Anwendungen immer nahtloser und immersiver machen. Es wird erwartet, dass der Markt für biometrische Authentifizierung bis zum Jahr 2026 8,79 Milliarden US-Dollar übersteigen wird. Gesichtserkennung und andere biometrische Verfahren werden in Verbraucheranwendungen immer häufiger eingesetzt, und die ständige Weiterentwicklung von FIDO-Protokollen („Fast ID Online“) wird das Wachstum auf den Märkten für mobile Unternehmensanwendungen weiter vorantreiben. Die zunehmende Integration von Spracherkennung in mobile Anwendungen ist unvermeidlich, da es für den Endbenutzer kaum Einfacheres gibt, als um etwas zu bitten. Dadurch müssen Nutzer ihre Telefone nicht mehr Hunderte von Malen am Tag entsperren.

Die Sprachtechnologie wird für Entwickler immer zugänglicher, und mit den Fortschritten in den Bereichen KI, natürliche Sprachverarbeitung (NLP, „Natural Language Processing“) und maschinelles Lernen muss die Sicherheit im Vordergrund stehen. Mobile Anwendungen mit Sprachschnittstellen werfen jedoch einige Bedenken in Bezug auf den Datenschutz (hört die Anwendung immer mit?) und die Sicherheit (wie wird das Gesagte sicher gespeichert?) auf. Die Datenschutz-Grundverordnung und andere Datenschutzgesetze weltweit werden sich mit diesem Trend weiterentwickeln müssen, um Sprachdaten genauso wie andere personenbezogene Daten zu schützen.

Wichtige Technologietrends mit Auswirkungen auf die Sicherheit mobiler Anwendungen

5G: Mit der zunehmenden Nutzung von Mobilgeräten und der Einführung der Cloud wächst das Volumen der ausgetauschten sensiblen Daten explosionsartig an. 5G-Kommunikationsnetze können nun höhere Datenübertragungsgeschwindigkeiten bei geringerer Latenz liefern. **Bis Ende 2024 wird es voraussichtlich 1,5 Milliarden 5G-Mobilfunknutzer geben und 5G wird 25 % des gesamten mobilen Datenverkehrs bewältigen.**[35] Das bedeutet natürlich, dass noch mehr sensible Daten ausgetauscht, übertragen und abgerufen werden, was wiederum zu noch mehr Daten führt, auf die es Cyberkriminelle abgesehen haben.

Mobile Zahlungen: In den letzten Jahren wurden Android- und iOS-Telefone zunehmend als Verkaufstellen-Terminals (PoS, „Point of Sale“) eingesetzt, was zu einem Boom bei der Einführung und Nutzung von kontaktlosen Zahlungen geführt hat. Der Umsatz mit mobilen Zahlungen erreichte im Jahr 2020 1,3 Billionen US-Dollar und für das Jahr 2021 wurden 1,7 Billionen US-Dollar erwartet.[36] Technologien wie NFC, Bluetooth und QR-Codes werden es Smartphones zunehmend ermöglichen, Zahlungsterminals und physische Geldbörsen zu verdrängen.



QR-Codes: Das Wiederaufleben von QR-Codes während der Pandemie hat uns in dem Glauben gelassen, dass ihre Verwendung nicht nur bequem ist, sondern dass sie aufgrund ihrer weiten Verbreitung auch harmlos sind. Mehr denn je verwandeln QR-Codes Produkte und Verpackungen in intelligente Produkte. Laut einer Umfrage von Statista werden **allein in den USA im Jahr 2020 schätzungsweise 11 Millionen Haushalte einen QR-Code gescannt haben.** Darüber hinaus gibt es in Asien, vor allem in China und Indien, eine deutlich höhere Akzeptanz.

Aber verschiedene Bedrohungsakteure nutzen QR-Codes als Angriffsvektor gegen Unternehmen und Privatpersonen. In den USA hat das Federal Bureau of Investigations (FBI) eine öffentliche Ankündigung vorgenommen, in welcher Mobiltelefonbenutzer vor der zunehmenden Zahl von Betrügereien und Angriffen gewarnt werden, die sich die zunehmende Verbreitung von QR-Codes zunutze machen.[37] Kriminelle Akteure manipulieren oder setzen ihre eigenen QR-Codes ein, um die Finanzinformationen oder wichtigen Daten eines Opfers zu stehlen und das Gerät durch bösartige Anwendungen zu kompromittieren.

Mobiles Cloud-Computing: Die mobile Cloud bezieht sich auf cloudbasierte Daten, Anwendungen und Dienste, die speziell für die Nutzung auf mobilen und anderen tragbaren Geräten entwickelt wurden. Im Jahr 2020 erreichte der Markt für mobile Clouds einen Wert von 30,71 Milliarden US-Dollar und es wird erwartet, dass er bis Ende 2026 118,70 Milliarden US-Dollar erreichen wird.[38] Die Kommunikation zwischen mobilen Geräten und Cloud-Diensten erfolgt bei diesen Anwendungen über ein drahtloses Netzwerk. Da wir uns nicht darauf verlassen können, dass die Sicherheit des mobilen Geräts jederzeit gewährleistet ist, ist die Sicherung von Daten, Schlüsseln und Cloud-Verbindungen innerhalb der Anwendung entscheidend.

Bei der Betrachtung der Ursachen für kritische Sicherheitsverletzungen im Zusammenhang mit mobilen Anwendungen fallen einige Muster auf:

App-Schwachstellen. Es kommt immer wieder vor, dass der Code von Entwicklern mobiler Anwendungen Daten von Mitarbeitern und Kunden preisgibt und damit den Datenschutz und die Sicherheit gefährdet. Zu den jüngsten Beispielen für kompromittierte Apps gehören die von „Ring Doorbell"-Kunden[39] genutzte mobile App, die Android-Version der Unternehmenskommunikationsanwendung Slack[40] und die Klarna-Zahlungs-App.[41]

Drittanbieter-Komponenten und -Entwickler. Entwickler von Mobilanwendungen werden immer abhängiger von Drittanbieter-Komponenten und Dienstleistungsanbietern, was erhebliche Risiken mit sich bringt. **Im Jahr 2021 wurden die privaten Daten von 21 Millionen Kunden der mobilen Park-App „ParkMobile" durch eine vom Unternehmen genutzte Drittanbietersoftware offengelegt.** Drittanbieterbibliotheken werden auch weiterhin in mobilen Anwendungen dominieren, da sie die Entwicklung vereinfachen, die Vermarktung beschleunigen und potentielle Kosteneinsparungen versprechen. Doch sie sind ein zweischneidiges Schwert. Sie erweitern die Angriffsfläche und erschaffen „überprivilegierte" Anwendungen – zwei Eigenschaften, auf die Cyberkriminelle insbesondere bei der Suche nach auszunutzenden Anwendungen achten.

Fehlkonfigurierte Clouddienste. Eine Untersuchung von 23 mobilen Anwendungen ergab, dass die Daten von mehr als 100 Millionen Nutzern offengelegt wurden.[42] Die Ursache? Es gelang den Entwicklern nicht, ihre Drittanbieter-Clouddienste korrekt zu konfigurieren. **Unsere Analyse von mehr als 1,3 Millionen Android- und iOS-Apps ergab, dass 131.000 von ihnen öffentliche Cloud-Dienste in ihrem Backend nutzten. 14 % dieser Apps wiesen Fehlkonfigurationen auf, durch die persönliche Daten der Nutzer offengelegt wurden.**[43]

> "Cyberspace is not a specific environment. In 2022, cyberspace has become a free fire zone with a multiplicity of actors. As the physical world and cyberspace have converged via smart phones; mobile malware, proximity attacks and application attacks are allowing for cybercriminals and spies to manifest in both your digital and physical life. From stealing your money; to turning on the microphone and camera specific to your location, to using your device to compromise your work network, cybercrime cartels have gone wireless. Security and safety are dependent on mobile security."
>
> **Tom Kellermann**
> *Head of Cybersecurity Strategy for VMware and Global Fellow for Cyber Policy at the Wilson Center*

Globale Bedrohung nach Regionen aufgeschlüsselt

Aus globaler Sicht lässt sich nicht leugnen, dass mobile Endgeräte vermehrt Bedrohungen ausgesetzt sind, die Unternehmensdaten und -dienste gefährden. Bei den Unternehmenskunden und den Risikodaten, die von den durch Zimperium weltweit gesicherten Android- und iOS-Geräten zurückgemeldet wurden, lassen sich mehrere Beobachtungen machen. Die Daten in diesen Diagrammen beziehen sich auf alle Bedrohungen und Risiken, die auf den von Zimperium gesicherten Unternehmensclients erkannt und abgewehrt wurden. Diese anonymisierten Unternehmensdaten umfassen auch erkannte Bedrohungen, die bei der Installation im Rahmen der Sichtbarkeitsstufe der Bereitstellung gemeldet wurden.

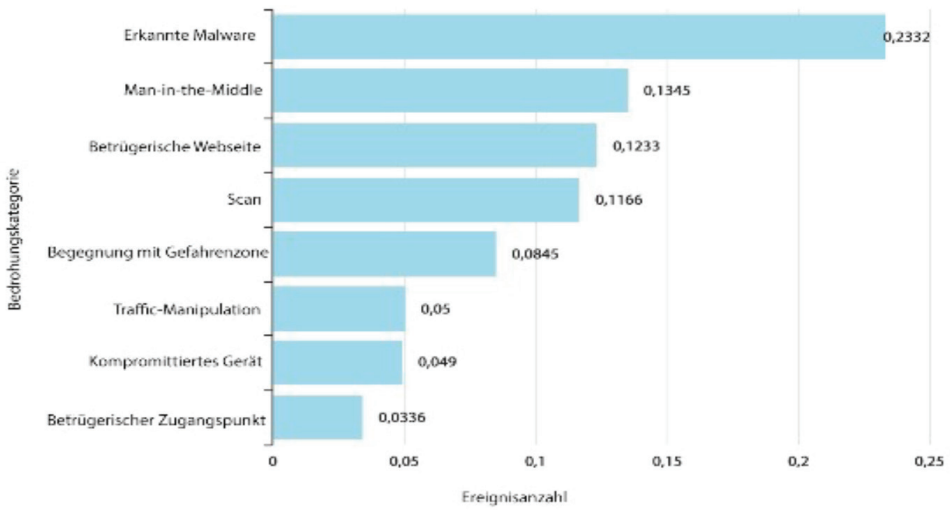
Unless stated otherwise, the following data and analysis is derived from the anonymized and aggregated data provided with permission to Zimperium from its enterprise clients.

Mobile Malware ist weiter verbreitet, als viele glauben. Im Jahr 2021 waren im weltweiten Durchschnitt 23 % der Endgeräte mit der einen oder anderen Form dieser bösartigen Anwendungen konfrontiert.

Unabhängig davon, ob sie von einem Drittanbieter oder direkt von einem OEM-Store heruntergeladen wird – Malware stellt das größte statistische Risiko für mobile Geräte, Benutzer und mit der Cloud verbundene Daten dar.

Ereignisse pro Jahr pro Gerät - **Globaler Durchschnitt**

Global Mobile Threat Events



Man-in-the-Middle-Angriffe und Scans stellten ebenfalls ein erhebliches Risiko für Endgeräte dar, da sie Teil größerer Angriffsketten gegen Unternehmenssysteme sowie wertvolle Datenzugriffe waren und als kritische Schritte in Angriffsketten für das Sammeln von Informationen und die Aufklärung dienten. Durchschnittlich 12 % der mobilen Endgeräte, das heißt 1 von 10, waren mit Phishing und bösartigen Webseiten konfrontiert, was ein Risiko für die Anmeldedaten der Benutzer, die Integrität der Geräte und die Unternehmenssicherheit darstellt.

23 % sind auf Malware gestoßen

13 % waren einem Man-in-the-Middle-Angriff ausgesetzt

12 % sind auf bößartige Webseiten gestoßen

12 % waren Scans ausgesetzt

8 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

5 % sind mit Traffic-Manipulation in Berührung gekommen

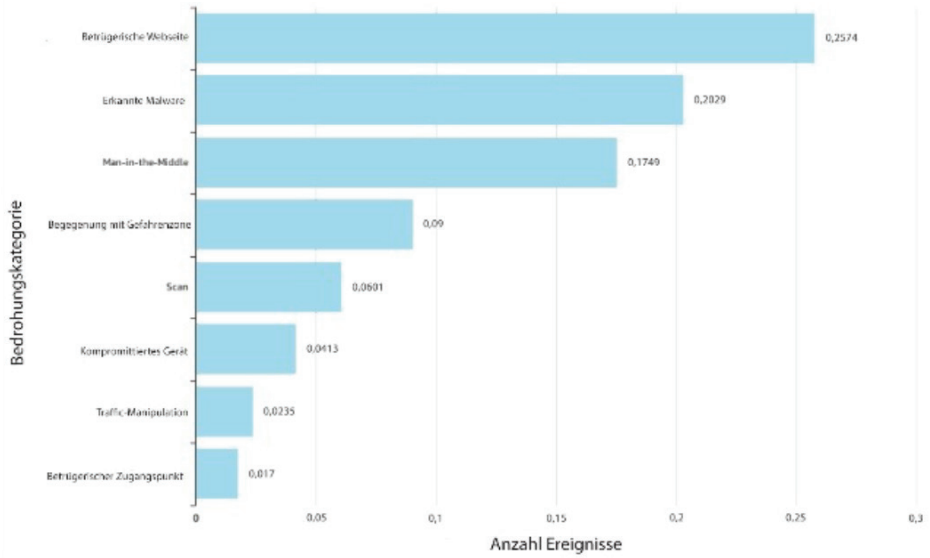
5 % kompromittierte Geräte

3 % waren mit einem betrügerischen Zugangspunkt konfrontiert

Bedrohungen für mobile Endgeräte, nach Region aufgeschlüsselt

Erwartete Ereignisse pro Jahr pro Gerät - Asien-Pazifik-Raum

Asia/Pacific, Mobile Threat Events (2021)



26 % sind auf bößartige Webseiten gestoßen

20 % sind auf Malware gestoßen

17 % waren einem Man-in-the-Middle-Angriff ausgesetzt

9 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

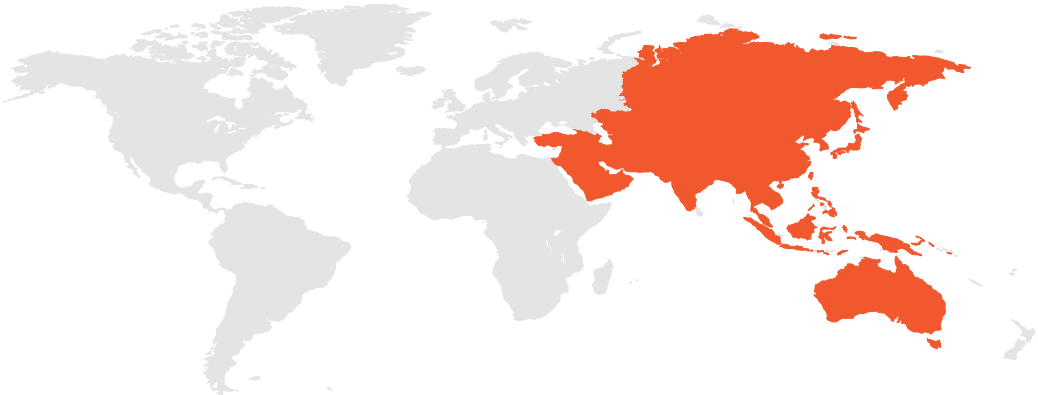
6 % waren Scans ausgesetzt

4 % kompromittierte Geräte

2 % sind mit Traffic-Manipulation in Berührung gekommen

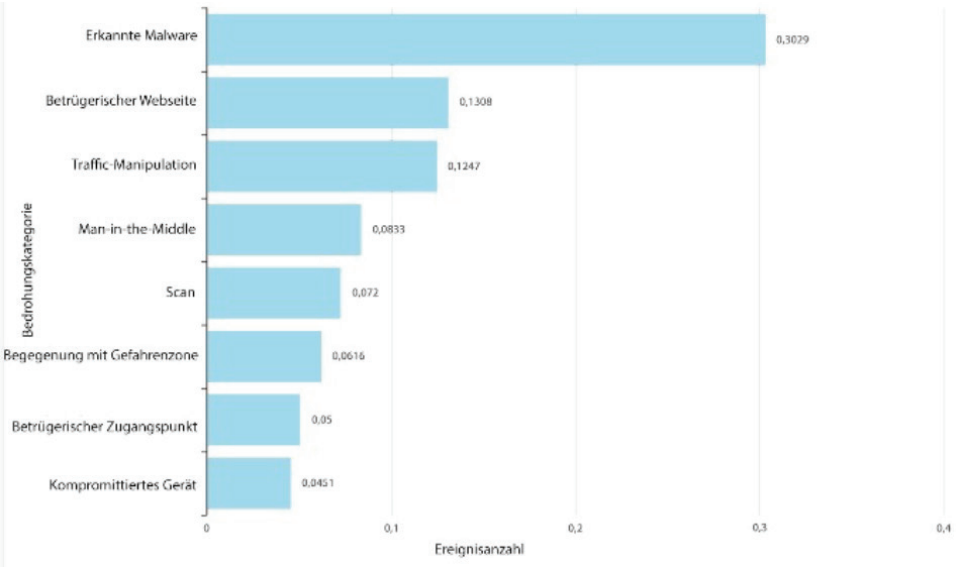
2 % waren mit einem betrügerischen Zugangspunkt konfrontiert

Asien/Pazifik – Die Wahrscheinlichkeit, dass mobile Nutzer in Asien auf bösartige Websites stoßen, ist doppelt so hoch wie im weltweiten Durchschnitt. 1 von 4 – oder 25 % – der mobilen Unternehmensgeräte wurde 2021 mindestens einmal mit Phishing konfrontiert. In der Region Asien/Pazifik dominierte das Phishing, das über gängige Kommunikationsmittel wie SMS, soziale Medien und andere Chat-Programme auf mobile Geräte abzielt. In-App-Nachrichten umgingen auch viele externe Sicherheitskontrollen und lieferten Phishing-Websites direkt auf das Mobilgerät. 1 von 5 Mobilgeräten wurde mit Malware infiziert, wobei die Hauptschuldigen nachweislich App-Stores von Drittanbietern und Sideloading durch Phishing waren. 17 % der durch Unternehmen gesicherten Mobilgeräte waren von Man-in-the-Middle-Angriffen betroffen, und bei knapp 10 % der Geräte wurden kritische Daten und Informationen von einem Netzwerk gescannt.



Erwartete Ereignisse pro Jahr pro Gerät - **Afrika**

Africa, Mobile Threat Events (2021)



30 % sind auf Malware gestoßen

13 % sind auf bößartige Webseiten gestoßen

13 % sind mit Traffic-Manipulation in Berührung gekommen

8 % waren einem Man-in-the-Middle-Angriff ausgesetzt

7 % waren Scans ausgesetzt

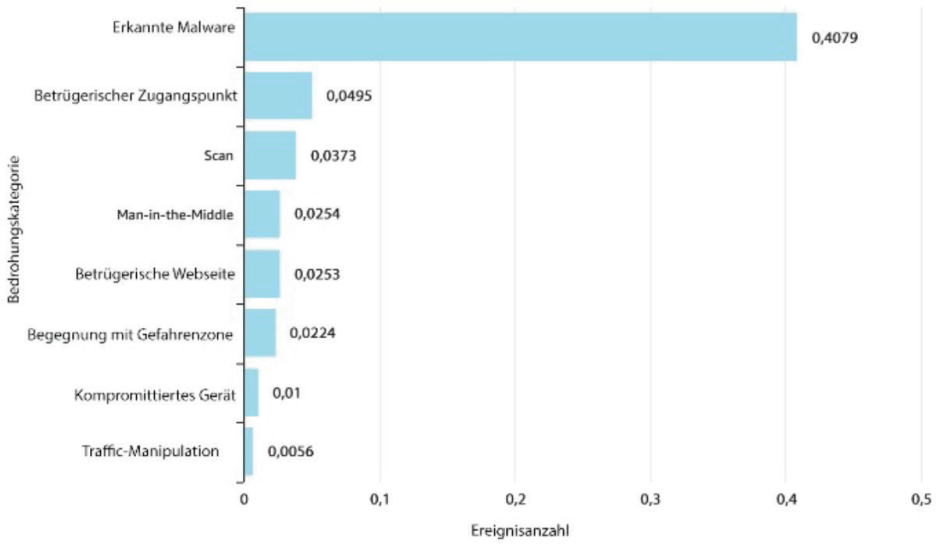
6 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

5 % waren mit einem betrügerischen Zugangspunkt konfrontiert

5 % kompromittierte Geräte

Afrika – Im Jahr 2021 waren überwältigende 30 % bzw. 1 von 3 mobilen Endgeräten in Afrika mit Malware infiziert, was das größte Risiko für Unternehmen und Nutzer in der Region darstellte. Phishing- und Spear-Phishing-Angriffe über SMS oder Kommunikationstools wurden auf 13 % oder etwas mehr als 1 von 10 mobilen Geräten entdeckt. Bei weiteren 13 % der Endgeräte kam es zu einer Manipulation des Datenverkehrs, die sich auf die tatsächliche Sicherheit der Verbindung des mobilen Geräts mit dem Netzwerk auswirkte. Etwa 8 % der Geräte sind mit riskanten Netzen verbunden. Diese Verbindungen stellen ein Risiko für die Kommunikation und die Daten durch Man-in-the-Middle-Angriffe dar.

Erwartete Ereignisse pro Jahr pro Gerät - Australien und Neuseeland



40 % sind auf Malware gestoßen

4 % waren mit einem betrügerischen Zugangspunkt konfrontiert

3 % waren Scans ausgesetzt

2 % waren einem Man-in-the-Middle-Angriff ausgesetzt

2 % sind auf bößartige Webseiten gestoßen

2 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

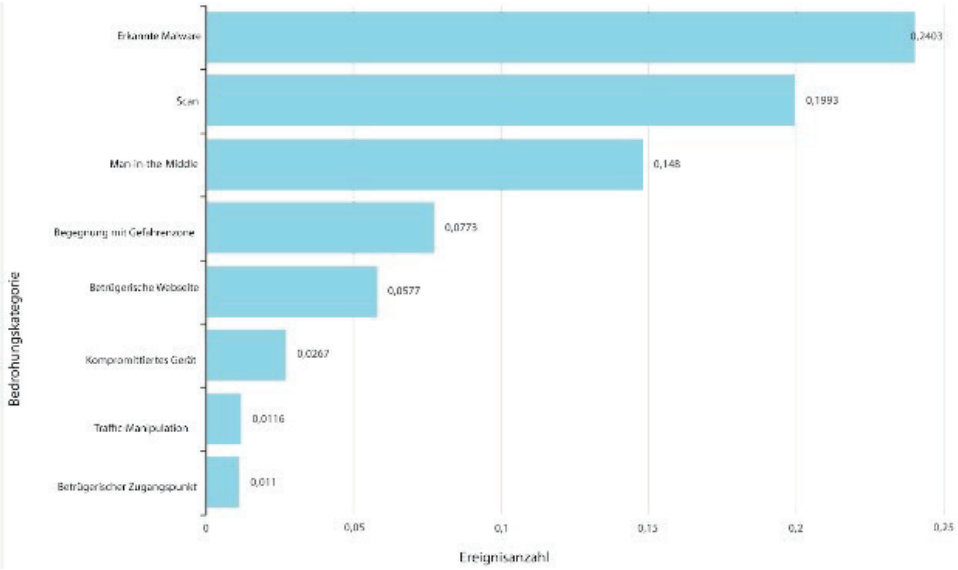
1 % kompromittierte Geräte

0,5 % sind mit Traffic-Manipulation in Berührung gekommen

Australien/Neuseeland – Die Wahrscheinlichkeit, dass Mobilfunknutzer in Australien und Neuseeland auf mobile Malware stoßen, ist fast doppelt so hoch wie im weltweiten Durchschnitt: 40 % der Geräte sind von bösartigen Anwendungen betroffen. Die Mobilfunknutzer in der Region sind auch häufiger als der weltweite Durchschnitt mit betrügerischen Zugangspunkten konfrontiert, wodurch Daten und Verbindungen gefährdet sind. In beiden Ländern waren Man-in-the-Middle-Angriffe und bösartige Websites mit 2 % der Nutzer, die diese Risiken auf mobilen Endgeräten sahen, gleichauf.

Erwartete Ereignisse pro Jahr pro Gerät - **Europe**

Europe, Mobile Threat Events (2021)



24 % sind auf Malware gestoßen

19 % waren Scans ausgesetzt

14 % waren einem Man-in-the-Middle-Angriff ausgesetzt

7 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

5 % sind auf bößartige Webseiten gestoßen

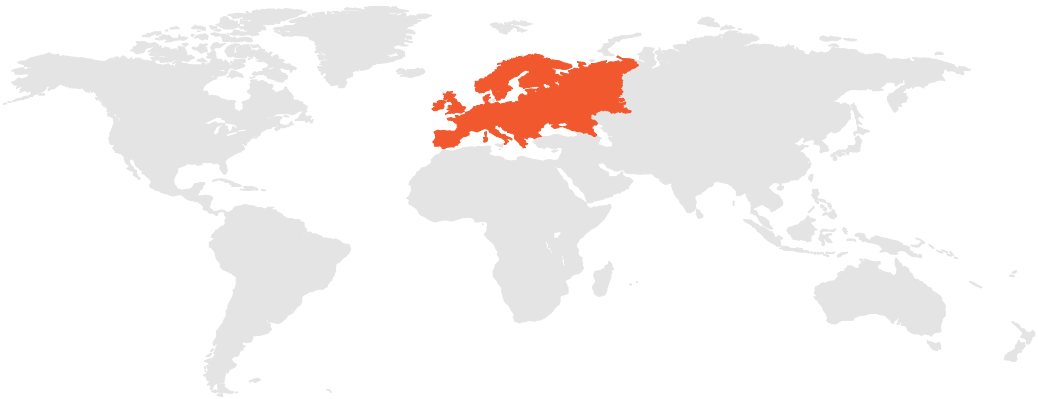
2 % kompromittierte Geräte

1 % sind mit Traffic-Manipulation in Berührung gekommen

1 % waren mit einem betrügerischen Zugangspunkt konfrontiert

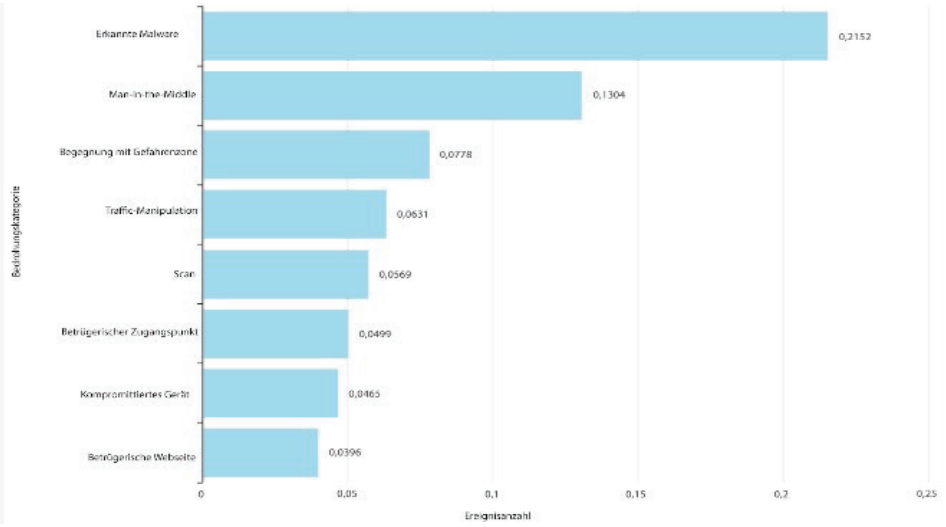
Europa – 1 von 4 bzw. 24 % der europäischen Mobilfunknutzer haben Malware auf ihren Geräten gefunden, wodurch persönliche und Unternehmensdaten gefährdet wurden.

Insgesamt stellten kompromittierte und böswillige Netzwerke sowie der Umgang mit Daten das größte Risiko für Mobilfunknutzer in den europäischen Ländern dar. 1 von 5 bzw. 19 % der Mobilfunknutzer wurden durch Scans in ihrem Netzwerk ausspioniert, wodurch möglicherweise wichtige Daten über das Gerät preisgegeben wurden. 14 % der Geräte wurden von Man-in-the-Middle-Angriffen heimgesucht und weitere 7 % verbanden sich mit Netzwerken, die hohe Risiken und Sicherheitsbedenken bargen.



Erwartete Ereignisse pro Jahr pro Gerät - Nordamerika

North American Mobile Threat Breakdown



22 % sind auf Malware gestoßen

13 % waren einem Man-in-the-Middle-Angriff ausgesetzt

8 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

6 % sind mit Traffic-Manipulation in Berührung gekommen

6 % waren Scans ausgesetzt

5 % waren mit einem betrügerischen Zugangspunkt konfrontiert

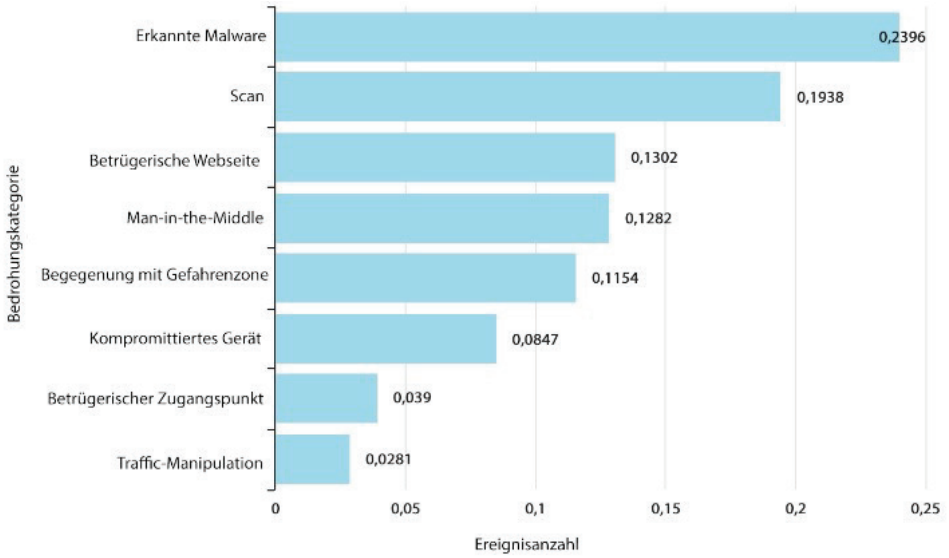
5 % kompromittierte Geräte

4 % sind auf bößartige Webseiten gestoßen

Nordamerika – Jedes vierte mobile Unternehmensgerät wurde in Nordamerika mit Malware infiziert, wodurch Geräte und Daten sowohl für den Endbenutzer als auch für das Unternehmen in Gefahr sind. Auch Man-in-the-Middle-Angriffe auf Telefone und Tablets waren mit einem Anteil von 13 % an den Versuchen, die Kommunikation abzufangen, auffällig. Obwohl sie nicht so ausgeprägt sind wie die beiden anderen Bedrohungen, zeigen die bekannten Risiken der böswilligen Netzwerk- und Datenverkehrsmanipulationen, dass Datenmanipulationen ein Unternehmensrisiko darstellen, das durch schlecht gesicherte Netzwerke entsteht.

Expected Events per Year Per Device | Südamerika

South America Mobile Threat Breakdown



24 % sind auf Malware gestoßen

19 % waren Scans ausgesetzt

13 % sind auf bößartige Webseiten gestoßen

13 % waren einem Man-in-the-Middle-Angriff ausgesetzt

12 % waren mit einem bekannten, bösartigen Netzwerk konfrontiert

8 % kompromittierte Geräte

4 % waren mit einem betrügerischen Zugangspunkt konfrontiert

3 % sind mit Traffic-Manipulation in Berührung gekommen

Südamerika – 1 von 4 mobilen Endgeräten bzw. 24 % der Endgeräte in Südamerika waren 2021 von mobiler Malware betroffen. Die Software wurde in der Regel entweder direkt aus den App-Stores heruntergeladen oder per Sideloading bereitgestellt, um regionale Beschränkungen zu umgehen. Bei 1 von 5 mobilen Geräten wurden Netzwerk-Scans durchgeführt, wodurch wichtige Geräteinformationen durch Angreifer gefährdet wurden. 13 % der Geräte in Südamerika, also etwas mehr als eines von zehn waren außerdem von Phishing- und Man-in-the-Middle-Angriffen betroffen, welche durch die Kommunikationsüberwachung oder den Diebstahl von Zugangsdaten wichtige Daten gefährdeten.

Diese Daten zeigen die Vielfalt der Risiken, Bedrohungen und Angriffe auf mobile Endgeräte auf globaler Ebene. Mobile Malware dominiert weiterhin die Bedrohungslandschaft und stellt die effizienteste und effektivste Methode dar, um mobile Endgeräte anzugreifen, zu kompromittieren und zu bestehlen. Auch netzbasierte Angriffe sind unglaublich effektiv und häufig, da sie sich eine wesentliche Eigenschaft von Mobiltelefonen zunutze machen – die Fähigkeit, immer eine Verbindung zu suchen. Angesichts der zunehmenden Zahl von Mitarbeitern und Kunden, die sich an verschiedenen Standorten befinden, müssen Unternehmen sich auf eine ständig im Fluss befindliche Bedrohungslandschaft vorbereiten und diese absichern, je nachdem, wo sich ihre Mitarbeiter, Anwendungen und Daten auf der Welt befinden. Die moderne Angriffsfläche ist gewachsen und die Bedrohungen für Unternehmen sind weiterhin vorherrschend und effektiv gegen ungesicherte Geräte.

Übersicht ausgenutzter Sicherheitslücken im Jahr 2021

„Das Wachstum mobiler Plattformen hat zu einem Anstieg der Produktanzahl geführt, für die beteiligte Personen Funktionen benötigen.“

- Maddie Stone & Clement Lecigne, Google Threat Analysis Group, 2021[45]

2021 war das „Jahr der Exploits“ Sicherheitsteams kämpften mit einer Zunahme von Zero-Day- und anderen, noch nie zuvor gesehenen Schwachstellen in Endgerätesystemen, einschließlich mobiler Android- und iOS-Systeme. **Die zunehmende Abhängigkeit vom mobilen Markt und dessen Wachstum haben böswilligen Akteuren die Möglichkeit eröffnet, typischerweise ungesicherte Systeme auszunutzen: Über 30 % der bekannten Zero-Day-Schwachstellen, die 2021 entdeckt wurden, betrafen mobile Geräte[44]. Dieser Trend stellt die größte Zunahme von Zero-Day-Exploits in der Geschichte von Smartphones und Tablets dar.** Sogar Googles Project Zero hat sich mit diesem Thema befasst, als kürzlich mehrere Zero-Day-Schwachstellen bekannt wurden.

Ob bekannt oder unbekannt, jeder Exploit stellt eine potenzielle Lücke in der Verwaltung der Angriffsfläche eines mobilen Geräts dar. In der Welt von BYOD-Richtlinien ist die Angriffsfläche für mobile Geräte nicht mehr nur eine Bedrohung für Verbraucher. Sie alle repräsentieren auch ein Risiko für die Unternehmenssicherheit. In den Händen der richtigen Angreifer kann jeder Exploit ein effektives Werkzeug für einen Angriff auf ein verwaltetes oder nicht verwaltetes mobiles Endgerät sein und dabei helfen, in Unternehmenssystemen und -netzwerken Fuß zu fassen.

Ungepatchte und unbehandelte bekannte Schwachstellen und Anfälligkeiten (CVE, „Common Vulnerabilities and Exposures“) stellen ein Risiko für Unternehmen dar, da sie Lücken in den Systemen hinterlassen. Um die Dinge noch komplizierter zu machen, verwalten die Hersteller ihre Sicherheitsupdatezyklen unterschiedlich. In der Zwischenzeit erhalten viele ältere Mobiltelefone nicht länger die neuesten Updates, so dass sie durch ältere bekannte Schwachstellen gefährdet sind und leichtere Ziele für kriminelle Akteure darstellen.

In den letzten Jahren ist die Erforschung von Zero-Day-Schwachstellen in mobilen Geräten immer lukrativer geworden. Vor diesem Hintergrund suchen immer mehr Forscher aktiv nach Exploits. Als Reaktion darauf müssen Unternehmen diese neuen Bedrohungen für ihre Systeme und Netzwerke entschärfen.

Da die Entdeckung mobiler Exploits für viele Sicherheitsforscher immer lukrativer wird, wurden mehr Zero-Day-Exploits entdeckt und gemeldet. Offizielle und inoffizielle „Bug-Bounties“ gibt es in Hülle und Fülle, mit hohen Auszahlungen für fortschrittliche Entdeckungen, zumindest im Vergleich zu Exploits für herkömmliche Endgeräte. Für bisher nicht gemeldete mobile Exploits bietet Zerodium, eine Plattform zum Erwerb von Exploits für erstklassige Zero-Days und fortschrittliche Cybersicherheitsforschung, derzeit Kopfgelder von bis zu 2.500.000 US-Dollar an.[46] Da Bounties für mobile Geräte den Forschern mehr als das Doppelte der Auszahlung einbringen können, handelt es sich um sehr wertvolle Untersuchungen.

Im Folgenden finden Sie eine Zusammenfassung der Schwachstellen von Android und iOS im Jahr 2021, welche die komplexen Angriffsflächen dieser beiden mobilen Ökosysteme verdeutlicht. Darin enthalten ist eine Übersicht der Zero-Day-Schwachstellen, die bei realen Angriffen auf mobile Geräte im Laufe der Geschichte der mobilen Endgeräte verwendet wurden.

Android-CVE-Tracker[47]

Laut der Schwachstellenverfolgung ist die Zahl der im Jahr 2021 entdeckten Schwachstellen für das Android-Betriebssystem mit 574 CVEs zurückgegangen. Im Jahr 2020 wurden insgesamt 859 entdeckt. Die häufigsten Schwachstellen waren Codeausführung, Systemumgehung und Überlauf von Code oder Speicher.

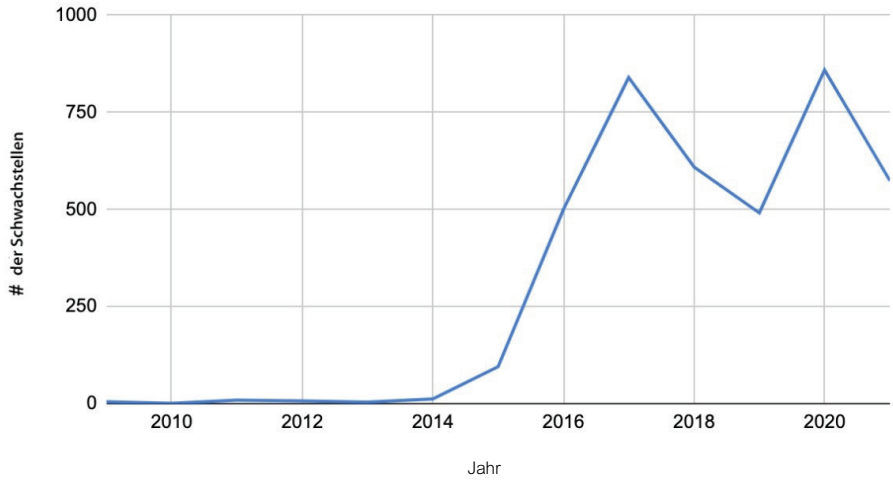
Von den gemeldeten und verfolgten Schwachstellen wurden:

21 % mit einer mittleren Angriffskomplexität eingestuft.

79 % mit einer niedrigen Angriffskomplexität eingestuft.

135 (**23** %) der bewerteten CVEs erhielten eine CVSS-Wertung von **7,2** oder höher, wobei **18** in die Kategorie "kritisch" fielen. Dies ist ein Rückgang gegenüber dem Vorjahr, mit im Jahr **2020 62** entdeckten und gemeldeten kritische Schwachstellen. **2020**.

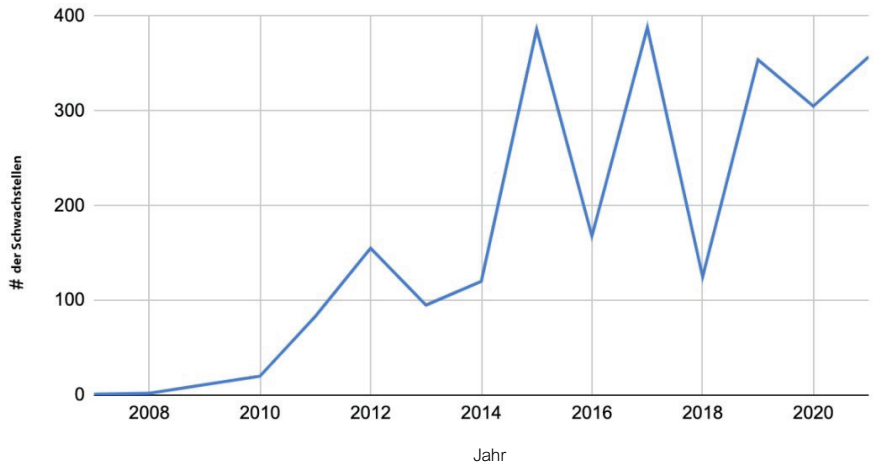
der Schwachstellen vs. Jahr



iOS-CVE-Tracker[48]

Laut der Schwachstellenverfolgung wurden Apple iOS im Jahr 2021 357 CVEs zugewiesen. Dies ist ein Anstieg gegenüber den 305 Entdeckungen und Meldungen im Jahr 2020. Die häufigsten Schwachstellen waren Codeausführung, gefolgt von Speicherverfälschung und Überlauf von Speicher oder Code.

der Schwachstellen vs. Jahr



Von den gemeldeten und verfolgten Schwachstellen wurden:

24 % mit einer niedrigen Angriffskomplexität eingestuft.

2 % mit einer hohen Angriffskomplexität eingestuft.

74 % mit einer mittleren Angriffskomplexität eingestuft.

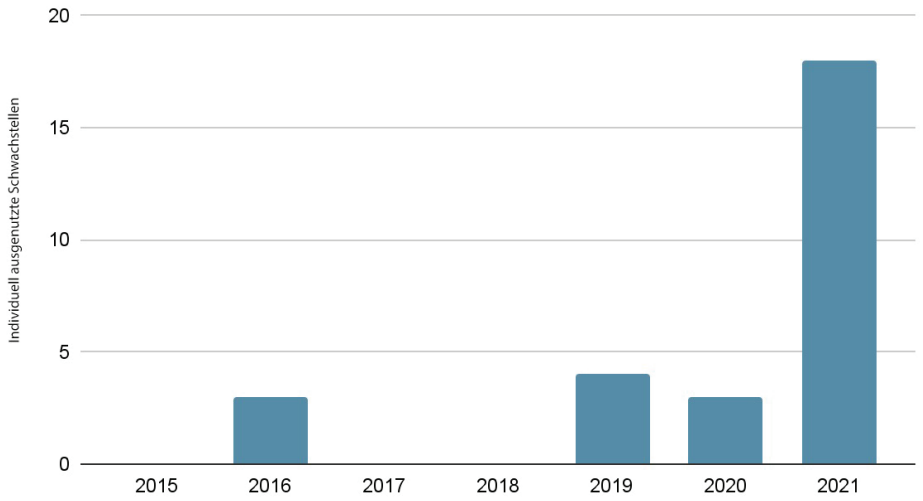
63 (**17** %) der bewerteten CVEs erhielten eine CVSS-Wertung von **7,2** oder höher, wobei **45** in die Kategorie "kritisch" fielen. Im Jahr **2020** wurden **67** kritische Schwachstellen ermittelt und gemeldet.

Im Jahr 2021 in freier Wildbahn entdeckte Zero-Day-Exploits[49]

Zero-Day-Exploits sind Schwachstellen, die bei tatsächlichen Angriffen auf Benutzer entdeckt wurden und bei denen weder die Öffentlichkeit noch der Hersteller von der Schwachstelle wusste. Dies bedeutet, dass zum Zeitpunkt des Angriffs kein Patch verfügbar war.

Das Jahr 2021 war das Jahr der mobilfunkspezifischen Zero-Day-Exploits, was sich in einem deutlichen Anstieg gegenüber den Vorjahren widerspiegelt.

Ausgenutzte Zero-Day-Schwachstellen in freier Wildbahn



Ein Blick auf die Trends gibt Aufschluss über die sich verändernde Landschaft der Zero-Day-Schwachstellen bei Mobilgeräten:

Im Jahr 2021 gab es einen 466-prozentigen Anstieg der ausgenutzten Zero-Day-Schwachstellen, die für aktive Angriffe auf mobile Endgeräte verwendet wurden.

- **2021:** 58 Zero-Day-Exploits insgesamt, davon 31 % (17) mobilgerätespezifisch
- **2020:** 26 Zero-Day-Exploits insgesamt, davon 11 % (3) mobilgerätespezifisch
- **2019:** 21 Zero-Day-Exploits insgesamt, davon 19 % (4) mobilgerätespezifisch

Trotz der enormen Beliebtheit mobiler Geräte in den letzten zehn Jahren haben sich in den letzten drei Jahren Zero-Day-Schwachstellen, die auf mobile Endgeräte wie Telefone und Tablets abzielen, zu einer größeren Herausforderung entwickelt als je zuvor.

Im Jahr 2021 entfielen 64 % der mobilgerätespezifischen ausgenutzten Zero-Day-Angriffe auf iOS-Schwachstellen.

Das Forschungsteam von zLabs führt diesen Anstieg auf die Zunahme persönlicher, privater und kritischer Datensysteme zurück, die mit mobilen Endgeräten verbunden sind. Wenn Angreifer nach neuen, ausnutzbaren Schwachstellen suchen, bevorzugen sie Geräte mit Datenzugang und geringer Sicherheitsabdeckung. Mobile Endgeräte stellen brauchbare Ziele dar, die der Schlüssel zum Datenreich werden, wenn man sie ausnutzt.

Der Aufstieg des Mobilgeräte-Phishings

Hinweise auf Phishing reichen bis ins Jahr 1995 zurück, doch statt als Fußnote der Geschichte vergessen zu werden, blieb diese Methode leider ein wichtiger Teil des Arsenals von Cyberangreifern. Im Großen und Ganzen funktioniert Phishing folgendermaßen:

- Kriminelle erstellen Webseiten, die etablierte Organisationen imitieren, und versuchen dann, Benutzer auf diese Webseiten zu locken.
- Wenn ein Benutzer seine Anmeldedaten oder vertraulichen Informationen an die Website übermittelt, kann der Angreifer diese Anmeldedaten verwenden, um die Kontrolle über Konten zu übernehmen oder andere Taktiken anzuwenden.
- Da viele Benutzer auf verschiedenen Webseiten dasselbe Passwort verwenden, kann ein erfolgreicher Angriff oft mehrere Dienste und Konten gefährden.
- Dabei wird Social Engineering genutzt, um das Vertrauen und die Neugier des Endbenutzers auf offiziell aussehende Mitteilungen auszunutzen.

Die Angreifer zielen in der Regel über elektronische Kanäle auf die Opfer ab, z. B. über E-Mail, Website-Hijacking und SMS-Nachrichten. Angreifer können jedoch auch Telefoninteraktionen nutzen, um ein Ziel zu täuschen. Im Laufe der Jahre haben sich verschiedene Unterkategorien herausgebildet:

- **Spear-Phishing.** Ein Angreifer, der es auf eine bestimmte Organisation oder Person abgesehen hat.
- **Whaling.** Angriffe auf hochrangige Führungskräfte und andere bedeutende Ziele.

Phishing continues to be employed because, quite simply, **it works.**

Phishing-Prävalenz

Phishing wird nach wie vor eingesetzt, weil es einfach funktioniert. Einem Bericht zufolge war Phishing bei 36 % der Sicherheitsverletzungen im Spiel, und zwischen 2020 und 2021 soll diese Praxis um 10 % zugenommen haben.[50] Weitere Untersuchungen ergaben, dass Phishing-E-Mails mit rund 54 % der Angriffe der wichtigste Einstiegspunkt für Ransomware sind.[51]

Auf die Frage nach den Risiken, die sie am meisten beunruhigen, war „Angriffe durch Phishing“ die meistgenannte Antwort (55 %). Darüber hinaus gaben 61 % der Befragten an, dass sie während der COVID-19-Pandemie einen Anstieg der Phishing-Angriffe beobachtet haben. Darüber hinaus wird die Erstellung von Phishing-Angriffen immer einfacher: Tools und Phishing-Kits ermöglichen es jetzt auch unerfahrenen Benutzern, mit wenigen Klicks betrügerische Websites zu erstellen.

gaben

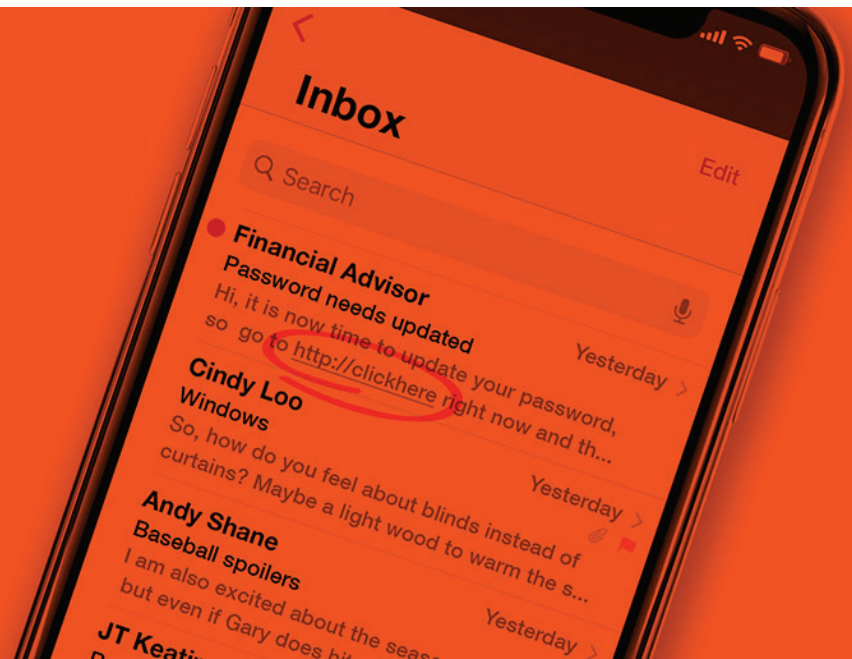
61%

der Befragten an, dass sie während der COVID-19-Pandemie einen Anstieg der Phishing-Angriffe beobachtet haben.

Im Laufe der Jahre haben wir uns immer mehr auf unsere Mobiltelefone verlassen, sowohl im privaten als auch im beruflichen Bereich. Dies war zwar schon seit einiger Zeit der Fall, aber die COVID-19-Pandemie hat den Übergang noch beschleunigt. Die zunehmende Nutzung von Smartphones bei der Arbeit bedeutet, dass die Nutzer routinemäßig auf Unternehmensressourcen und -anwendungen zugreifen. Dies und die Tatsache, dass diese Geräte nicht über das gleiche Sicherheitsniveau verfügen wie herkömmliche Laptops und Desktops, ermutigt potenzielle Angreifer, sich auf Mobilgeräte zu konzentrieren.

Mobile Endgeräte verfügen in der Regel über keinerlei Sicherheitsvorkehrungen, und wenn doch, dann sind diese Sicherheitsmechanismen in der Regel nicht auf demselben Niveau wie bei herkömmlichen Endgeräten. Wenn Teams versuchen, herkömmliche Sicherheitstools auf mobile Geräte anzuwenden, stoßen sie häufig auf mehrere Einschränkungen. So können beispielsweise Verarbeitungseinschränkungen die potenziellen Analysemöglichkeiten begrenzen. Auf mobilen Geräten liefern Sandboxing-Tools nicht alle Informationen, die für eine erweiterte Bedrohungserkennung erforderlich sind.

Außerdem stellen mobile Geräte naturgemäß zusätzliche Herausforderungen dar. Die kleineren Bildschirme mobiler Endgeräte können Anhaltspunkte verbergen, die einen Benutzer auf eine bösartige Website aufmerksam machen könnten, da die Bildschirmgröße Warnhinweise überdecken kann. Mobile Geräte werden für viele Kommunikationsvektoren verwendet, darunter E-Mail, Chat, In-App-Messaging, Instant Messaging und mehr. Diese verschiedenen Kanäle bieten Kriminellen eine wachsende Zahl von Angriffsflächen.



Wenn man die Sicherheitsmängel mobiler Geräte mit der Tatsache verbindet, dass diese Geräte nun als Schnittstellen zu sensiblen Unternehmens- und Privatdaten fungieren, ist es nicht verwunderlich, dass sie zunehmend in den Fokus von Angreifern geraten.

Während Phishing früher überwiegend geräteunabhängig war, hat Zimperium eine Zunahme von Phishing-Websites festgestellt, die speziell auf Mobiltelefone zugeschnitten sind. Wir haben über einen Zeitraum von zweieinhalb Jahren eine Analyse unserer und öffentlich zugänglicher Daten durchgeführt. Für diese Analyse haben wir mehr als 500.000 Seiten untersucht. **In diesem Zeitraum wuchs die Anzahl der auf Mobilgeräte zugenschnittenen Phishing-Webseiten um 50 %. Darüber hinaus zielten im Jahr 2021 75 % der analysierten Phishing-Websites speziell auf Mobilgeräte ab und lieferten für das mobile Format geeignete Inhalte.**

Phishing-Seiten, die Schwachstellen in Mobilgeräten ausnutzen 2019-2021

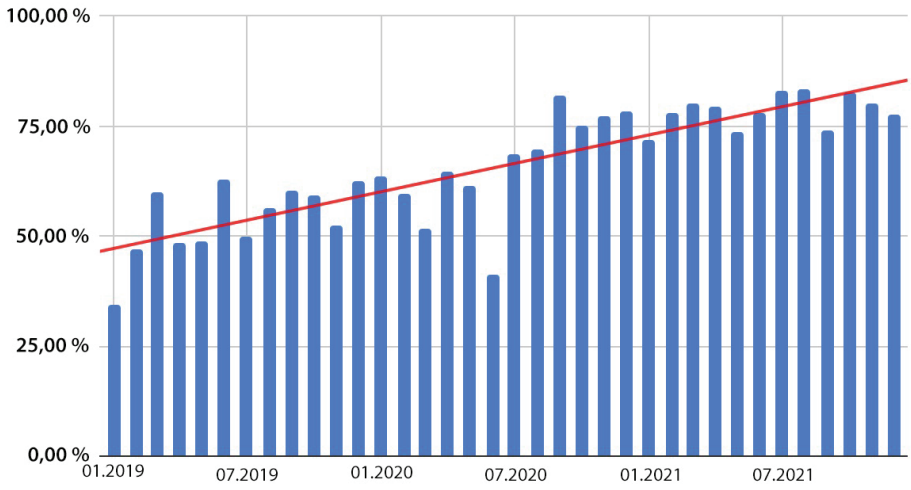


Abbildung #: Die Zahl der Phishing-Websites, die speziell auf mobile Geräte abzielen, hat rapide zugenommen und mittlerweile machen diese mehr als drei Viertel aller analysierten Websites aus.

Darüber hinaus werden die verfolgten Angriffe immer ausgefeilter. **Zwischen 2019 und 2021 stieg beispielsweise der Anteil der Phishing-Seiten, die eine sichere Kommunikation (allgemein als HTTPS bekannt) nutzen, stetig an, wodurch es für die Nutzer immer schwieriger wurde, diese Seiten von seriösen Seiten zu unterscheiden.**

Phishing-Seiten, welche HTTPS nutzen 2019-2021

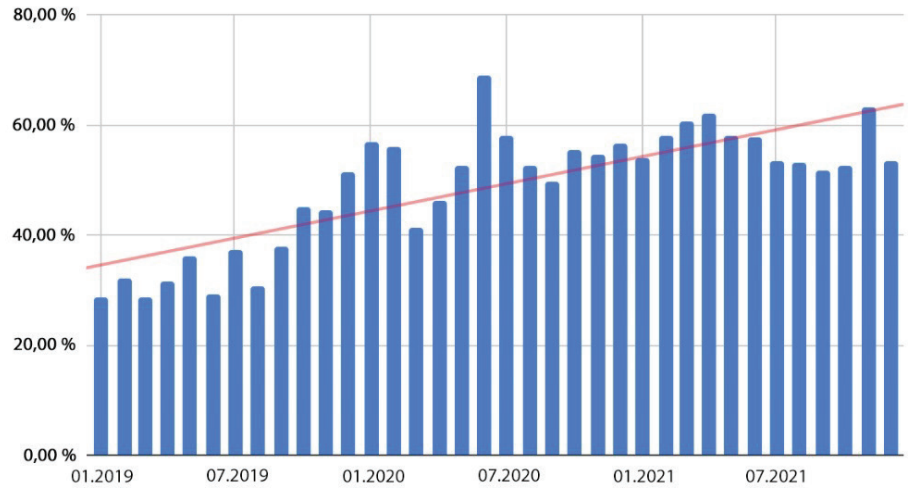


Abbildung #: Der Prozentsatz der Phishing-Webseiten, die das HTTPS-Protokoll verwenden, ist stetig gestiegen.

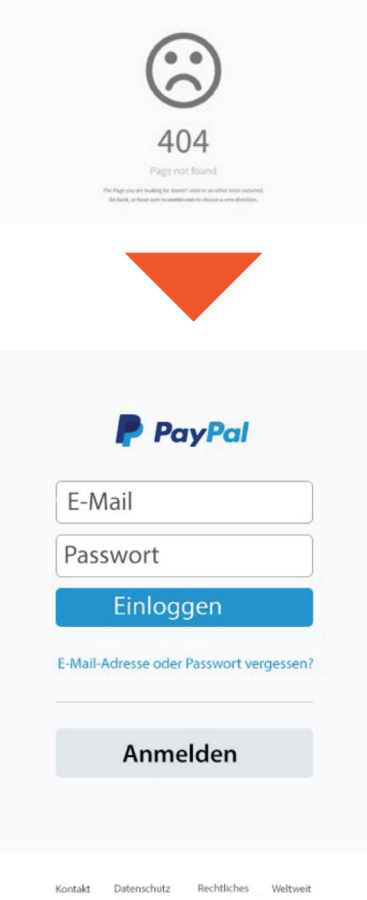


Abbildung #: Während ein Nutzer, der diese Malware-Webseite mit einem Laptop aufruft, eine 404-Fehlermeldung erhält, wird dem Benutzer eines Mobilgerätes eine Phishing-Webseite angezeigt, die den Anmeldebildschirm von PayPal imitiert.

Wie Angreifer Mobilgeräte ins Visier nehmen

Um mobile Geräte zu schädigen, verwenden Angreifer entweder adaptive oder responsive Techniken. Hier finden Sie eine Zusammenfassung einiger dieser Methoden.

Adaptive Webseiten

Adaptive Websites können je nach verwendetem Gerät völlig andere Inhalte laden und auf andere Websites umleiten. Angreifer passen die Inhalte auf Grundlage des Benutzers des mobilen Endgeräts an. Auf diese Weise kann ein Angreifer exklusiv auf Mobilgeräte abzielen. Wenn beispielsweise ein Desktop erkannt wird, können sie verhindern, dass die Seite überhaupt geladen wird. Auf diesem Weg können Angreifer die Entdeckung durch Desktops mit Bedrohungserkennungswerkzeugen vermeiden.

Responsive Webseiten

Responsive Websites passen die Platzierung und Größe von Objekten an die Bildschirmgröße des verwendeten Endgeräts an und zeigen dem Betriebssystem entsprechende Dialogschnittstellen an. Während diese Reaktionsfähigkeit es legitimen App-Entwicklern ermöglicht, eine bessere Benutzererfahrung zu bieten, können dieselben Fähigkeiten Angreifern einen Vorteil beim Phishing verschaffen.

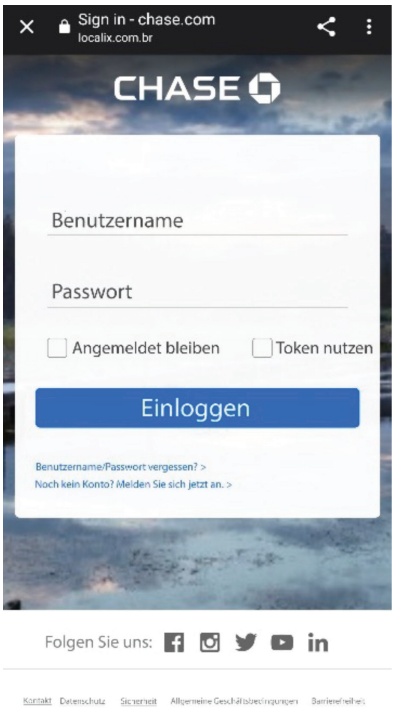


Abbildung #: Beispiel der Ansicht, welche ein Mobilgerätenutzer von der gleichen Phishing-Seite erhalten würde.

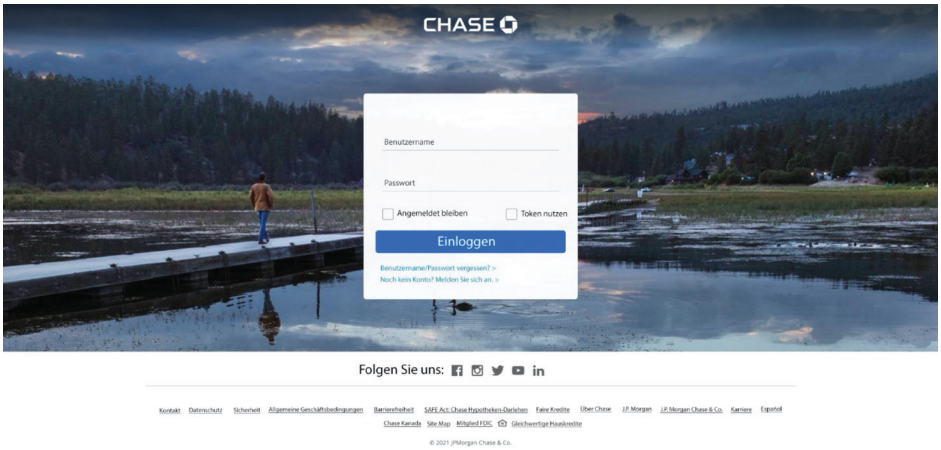


Abbildung #: Ein Beispiel für eine responsive Phishing-Webseite, die auf Kunden von Chase abzielt. Diese Ansicht würde ein Desktop-Benutzer erhalten.

Die häufigsten für Phishing genutzten Marken, Weltweit

Bei Phishing-Angriffen versuchen Kriminelle, ihren Opfern vorzugaukeln, sie seien im Kontakt mit einem Unternehmen, mit dem sie regelmäßig Geschäfte machen. Daher ist es nicht verwunderlich, dass es eine klare Korrelation gibt zwischen der Popularität einer Marke und der Tendenz, sie für kriminelle Zwecke zu missbrauchen. **Die bekanntesten, auf den Verbraucher ausgerichteten Institutionen aus den Bereichen Einzelhandel, soziale Medien, Technologie und Finanzdienstleistungen dominieren die Phishing-Kategorie. Phisher hoffen, dass das Vertrauen eines Verbrauchers in eine bestimmte Marke ihn dazu bringt, seine Anmeldedaten zu übermitteln.** Nachfolgend sind die regionalen Ergebnisse in Bezug auf die von Phishern am häufigsten verwendeten Marken aufgeführt.

Nordamerika

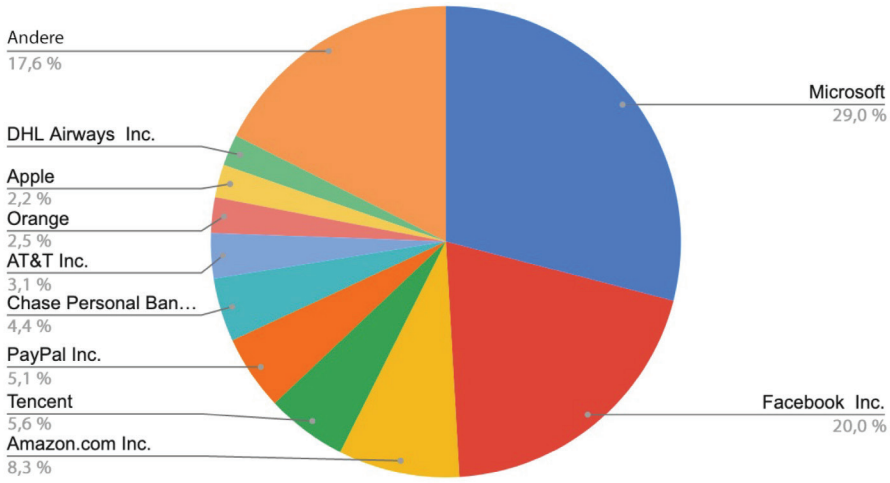


Abbildung #: Der Prozentsatz der Unternehmen, die von Phishing-Seiten imitiert werden, welche auf Nutzer in Nordamerika abzielen.

In Nordamerika gab fast ein Drittel (29 %) der Phishing-Angriffe auf Unternehmen vor, von Microsoft zu stammen. Auf Phishing-Seiten, die Microsoft und Facebook (20 %) nachahmen, entfiel fast die Hälfte aller Angriffe. Amazon lag mit etwas über 8,3 % auf einem abgeschlagenen dritten Platz. Zu den übrigen Webseiten gehörten auch Finanzdienstleister (PayPal und Chase zusammen 9,5 %), Telekommunikationsunternehmen (AT&T 3,1 % und Orange 2,5 %) und ein Versandunternehmen (DHL Airways 2,2 %).

Mittel- und Südamerika

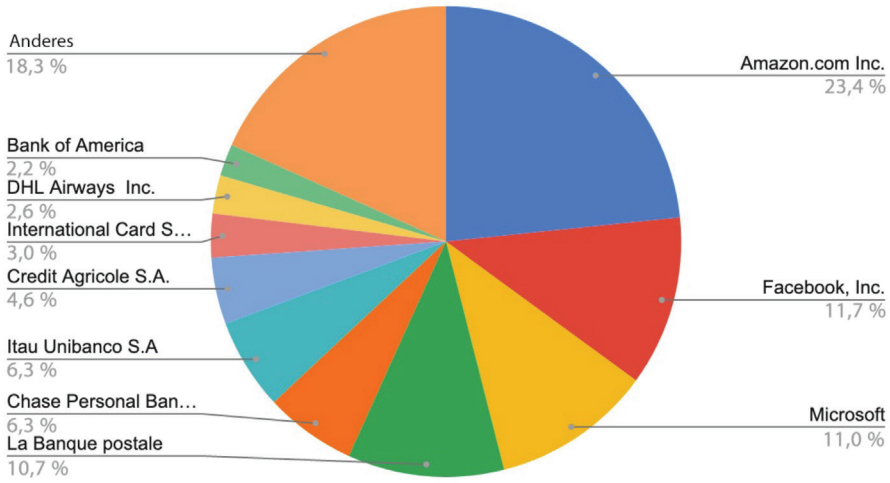


Abbildung #: Der Prozentsatz der Unternehmen, die von Phishing-Seiten imitiert werden, welche auf Nutzer in Mittel- und Südamerika abzielen.

In Mittel- und Südamerika wurden Microsoft und Facebook, die Nummer eins und zwei in Nordamerika, von Amazon verdrängt, das auf fast einem Viertel (23,4 %) aller Phishing-Seiten imitiert wurde. Facebook und Microsoft belegten die Plätze zwei und drei. Mit Ausnahme von DHL Airways (2,6 %) handelte es sich bei den übrigen Top-Phishing-Marken um Finanzdienstleister, wobei La Banque Postale in 10,7 % der Angriffe auftauchte.

Europa/Nahost

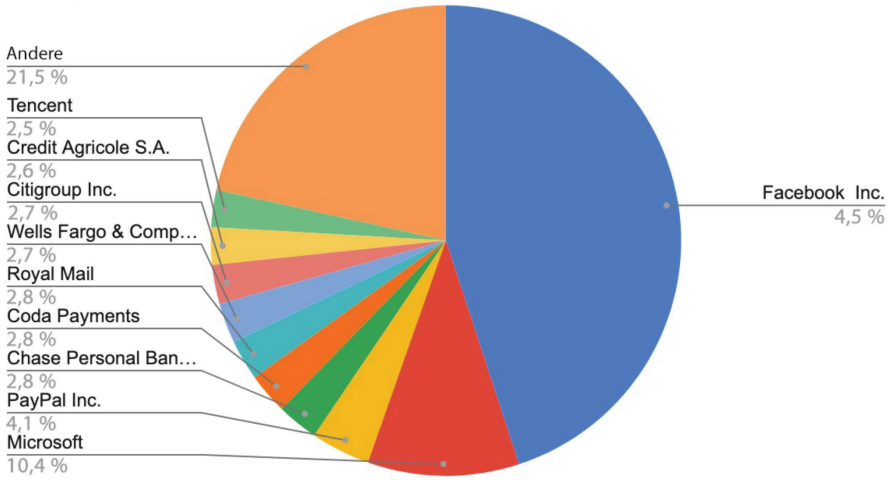


Abbildung #: Der Prozentsatz der Unternehmen, die von Phishing-Seiten imitiert werden, welche auf Nutzer in Europa und Nahost abzielen.

In Europa und Nahost ist Facebook mit Abstand die beliebteste Marke für Phishing-Angriffe. Auf das Social-Media-Unternehmen entfielen 45 % der unternommenen Angriffe. Microsoft lag mit 10,4 % weit abgeschlagen an zweiter Stelle. Bei sechs der neun verbleibenden, am häufigsten betroffenen Marken waren Finanzdienstleister das Ziel.

Afrika

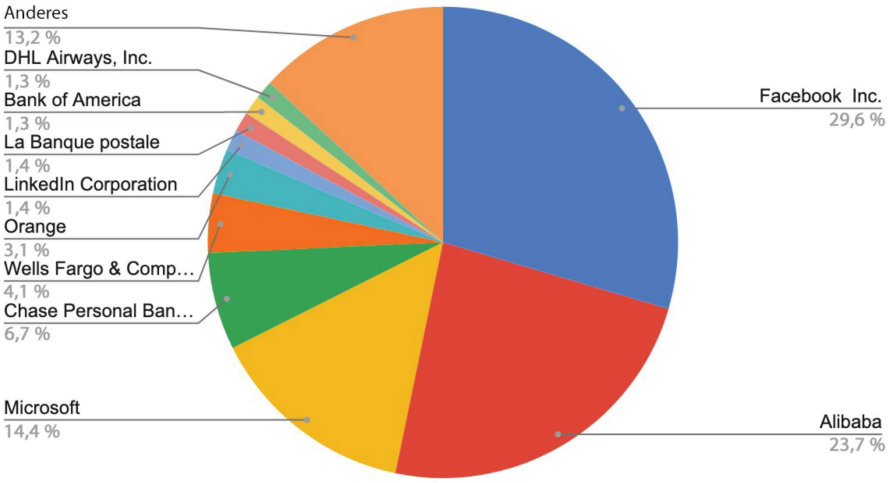


Abbildung #: Der Prozentsatz der Unternehmen, die von Phishing-Seiten imitiert werden, welche auf Nutzer in Afrika abzielen.

In Afrika, wie auch in Europa und Nahost, war Facebook die erste Wahl von Angreifern und wurde auf 29,6 % der Phishing-Seiten verwendet. Der große Marktanteil von Alibaba in Afrika spiegelte sich im Ergebnis wider und umfasste 23,7 % der Angriffe. Microsoft (14,4%) lag auf Platz drei, gefolgt von Chase (6,7%) und Wells Fargo (4,1%).

Australien

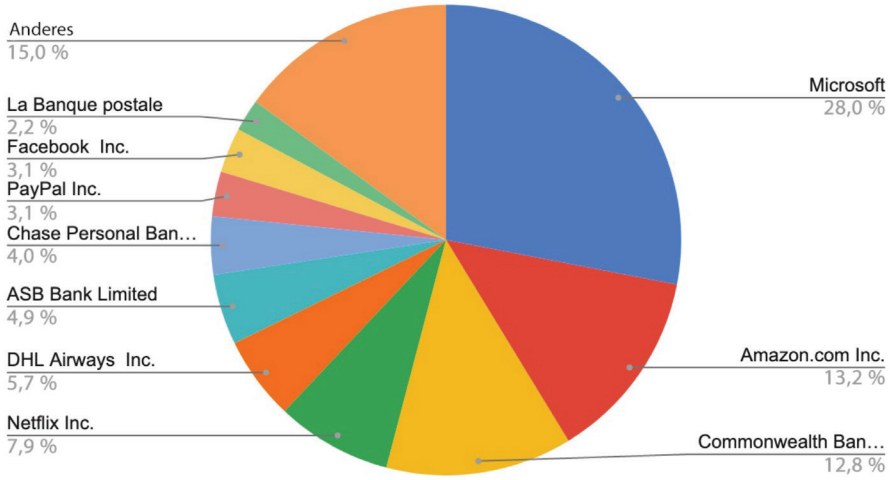


Abbildung #: Der Prozentsatz der Unternehmen, die von Phishing-Seiten imitiert werden, welche auf Nutzer in Australien abzielen.

Wie in Nordamerika ist auch in Australien Microsoft die am häufigsten betroffene Marke und taucht auf 28 % der Phishing-Seiten auf. Auf Amazon (13,2 %) und die Commonwealth Bank (12,8 %) folgte mit Netflix (7,9 %) eine Marke, die in anderen Regionen nicht annähernd so stark vertreten war. Neben Commonwealth waren mehrere Finanzdienstleister in den Top 10 vertreten, darunter ASB Bank (4,9 %), Chase (4,0 %), PayPal (3,1 %) und La Banque Postale (2,2 %).

Asien/Pazifikraum

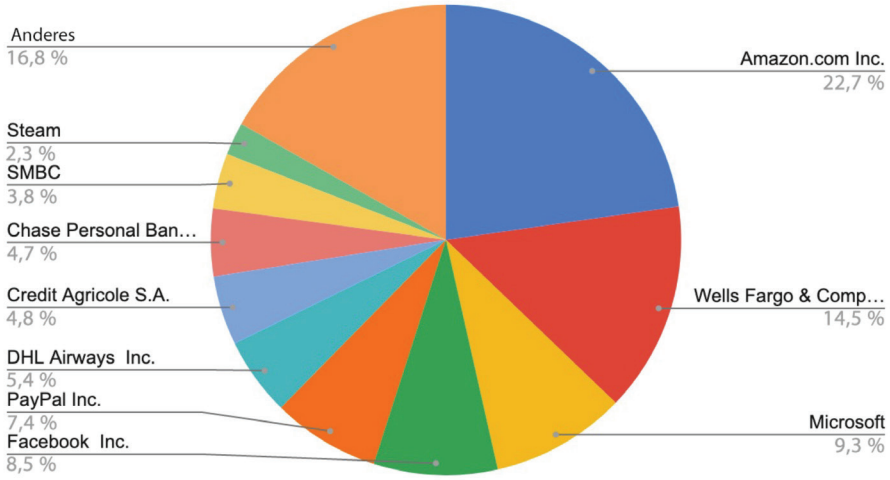


Abbildung #: Der Prozentsatz der Unternehmen, die von Phishing-Seiten imitiert werden, welche auf Nutzer in Asien/dem Pazifikraum abzielen.

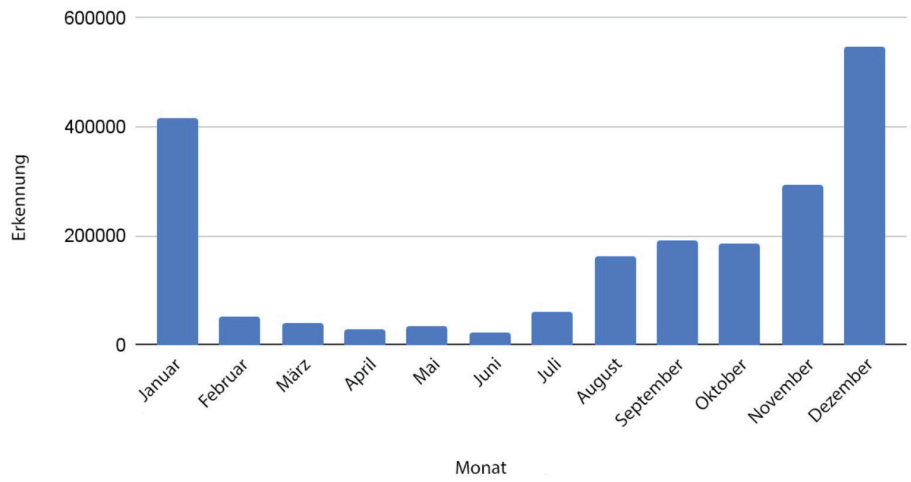
In der Region Asien-Pazifik war Amazon (22,7 %) die von Phishern am häufigsten verwendete Marke. Wells Fargo ist zwar in mehreren Regionen vertreten, hier aber mit 14,5 % am stärksten vertreten. Obwohl Steam in diesem Bereich eine dominante Marktposition innehat, wurde es nur bei 2,3 % der Angriffe eingesetzt.

Risiken und Angriffe – Mobile Malware, Bugs und Profile

Malware gehört zum Arsenal eines jeden Angreifers, denn sie ist leicht zugänglich, einfach zu installieren und kann in großem Umfang Schaden anrichten. Es gibt Millionen verschiedener Malware-Stämme, und täglich werden Tausende neuer Programme entwickelt und veröffentlicht. Malware ist zur größten Profitquelle für die Täter geworden, und aus diesem Grund ist sie ein sich ständig veränderndes Ziel.

Im Jahr 2021 entdeckte die mobile Sicherheitsanalyse von Zimperium 2.034.217 neue Malware-Samples in freier Wildbahn. Im Durchschnitt sind das fast 36.000 neue Malware-Stämme pro Woche und über 5.000 pro Tag.

Neue Android-Malware-2021



Obwohl die Zahl neuer Malware im Vergleich zum Vorjahr um 50 % gesunken ist, deuten unsere Ergebnisse darauf hin, dass auch wiederverwendete Malware-Familien zu dieser Veränderung beitragen. Die Forscher stellten außerdem fest, dass Angreifer in den vergangenen Jahren stark in ausgefeilte Frameworks wie Flutter, Cordova und Unity investiert haben, statt in herkömmlichen Code.

Im Jahr 2020 nutzten Angreifer die durch die Pandemie bedingten Lockdowns, welche Unternehmen weltweit dazu zwangen, ihre Mitarbeiter dezentral einzusetzen.

Im Jahr 2020 nutzten Angreifer die durch die Pandemie bedingten Lockdowns, welche Unternehmen weltweit dazu zwangen, ihre Mitarbeiter dezentral einzusetzen. Diese neuartigen Situationen stellen eine wesentlich größere Angriffsfläche dar, da die Mitarbeiter häufig sowohl firmeneigene als auch private Geräte, wie z. B. Mobilgeräte, verwenden, um effizient zu arbeiten. Letztlich hat diese Situation zu einer Zunahme von Malware, Ransomware und Exploits in Unternehmen geführt.

Im Jahr 2021 zeigten unsere Daten, dass neue mobile Malware-Varianten ab Oktober zunahmen und im Dezember einen Höhepunkt erreichten. Dieser Anstieg war keine Überraschung. Kriminelle nutzen Online- und Einzelhandelsrabatte, die über Links in E-Mails und Textnachrichten während der Feiertage beworben werden, in der Hoffnung, dass die Benutzer Malware über ihre Mobiltelefone herunterladen.

Mobile Malware ist einzigartig, weil die mobile Angriffsfläche anders ist. Einige Varianten mobiler Malware verhalten sich wie herkömmliche Endgeräteangriffe, etwa Spyware und Trojaner. Andere Malware kann die Nutzer auf eine Weise beeinträchtigen, wie es herkömmliche Malware nicht kann, z. B:

- Diebstahl von 2FA-Daten
- Durchführung von Overlay-Angriffen
- Angriff auf andere Mobilanwendungen
- Standorttracking des Nutzers
- Aufzeichnung persönlicher Audiodaten
- Zugriff auf private Fotos und persönliche Daten
- Verfolgung von Sensordaten

Um Erkennungsmechanismen zu umgehen und die sprichwörtliche goldene Gans nicht zu töten, werden Umgehungs- und Exploit-Techniken entwickelt, wie die Anzahl neuer mobiler Malware-Samples beweist, die wir täglich sehen. Nicht nur ist die Erkennung mobiler Malware schwierig, Mobilgeräte sammeln auch große Mengen wertvoller Daten. Dies ist ein ideales Umfeld für Kriminelle, die einen schnellen und lukrativen Angriff durchführen wollen.

Advanced Novel Malware Techniques Targeting Mobile

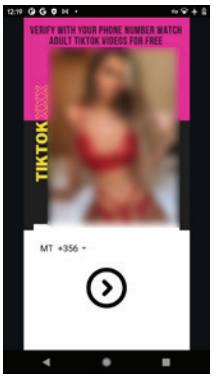
Mobile malware is following the path of traditional, advanced attacks in what can almost be described as a renaissance period. New and advanced capabilities are making their way into the mobile attack chain, taking advantage of the new capabilities, constant data access, and lack of security across the ecosystems. Past samples of mobile malware were often viewed as simple and granular, but recently discovered samples of mobile malware and attacks show complicated techniques used in targeting traditional endpoints and services are starting to make their way into mobile attacks.

Die vergrößerte Angriffsfläche von Apples iOS-Geräten

Im Jahr 2021 enthüllte Apple eine beliebte iOS-Funktion, die es Unternehmen ermöglichte, Anwendungen von außerhalb des App Stores zu installieren und vergrößerte damit unbeabsichtigt den Angriffsvektor von iOS-Geräten, ohne dass es eine Möglichkeit gab, die Angriffe zu verhindern.

Diese iOS-Konfigurationsprofile bieten Unternehmen eine detaillierte Kontrolle über iOS-Geräte, ohne dass die Einreichung im App Store von Apple überprüft werden muss. Nach der Genehmigung stellt Apple ein signiertes Zertifikat zur Verfügung, welches das Unternehmen auf das Endgerät aufspielen und so jede selbst erstellte App darauf installieren kann. Diese Funktion ermöglichte es den Endbenutzern jedoch auch, nicht genehmigte und oft ungesicherte Anwendungen ohne etablierte OEM-Schutzmaßnahmen zu laden, was das Risiko von Datendiebstahl und -missbrauch auf dem Gerät erhöhte.

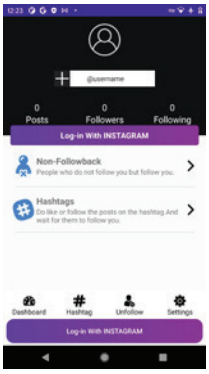
Aus dem von Apple im Oktober 2021 veröffentlichten Bericht geht hervor, dass Bedrohungsakteure dieses Programm seit Jahren missbrauchen. Sie nutzen es, um Malware, Spyware und andere bösartige Anwendungen auf Geräte zu verteilen und zielen damit auf Benutzer und Unternehmen weltweit.

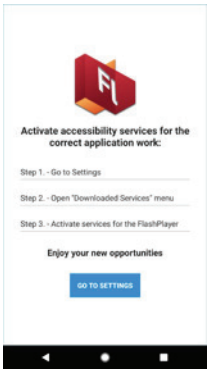


2FA Interception

Sample: 4a7d9ee4d3a7132d2838a78a8744522b5324c7267fa2675ab70e36b73ceecf

Disguised as an adult version of TikTok. After installation, it asks for the user's phone number and immediately sends it to the C&C. The backend starts generating login attempts for a series of services, like Telegram, Google, AliPay, Amazon, MPL, Ludo, Viber, and as well as various Russian services. The app is then responsible for intercepting the 2FA codes. The codes are then sent back to the C&C, completing the account takeover.





Persistent Attacks

Sample: ed4a7d9ee4d3a7132d2838a78a8744522b5324c7267fa2675ab70e36b73ceecf

A new variation of a classic banker trojan, this app mimics a flash player but doesn't have any function. This advanced mobile malware heavily relies on the TOR network to anonymously deliver a malicious payload and communicate with the C&C. The flow of the attack starts with the extraction and execution of the payload in memory (no traces on disk). Afterward, the app downloads the TOR binaries for the specific architecture, requesting the C&C address via the TOR network, and downloads the overlay payload from the C&C.
From there, additional APK payloads are downloaded, leading to an overlay attack on 238 target applications with the capability to dynamically add support for additional targets. It aggressively asks for accessibility services and cannot be uninstalled or opened again. There is no way to remove the malware after installation and requires a factory reset of the device.

Credential Theft

Sample: 1f403159ec3c5e1f1ef739ca01f5eff76d3fdfe1d8b7dd40d75de9cf30506958

This credential stealing app disguises itself as an Instagram follower tool. In actuality, it is a Facebook credential stealer, getting the cookies after a legit login attempt.

Sample: 5d065ed8c31e32041120722db9f3b7c24225e07935c720efe345ffd1e86b-d8ce targets

Facebook credentials, injecting malicious JavaScript in the displayed WebView to intercepts a victim's credentials. Credential theft mobile malware is on the rise due to the common practice of reusing passwords across multiple services, giving attackers access to various tools and logins.

Apple iOS's Increased Attack Surface

It is not just malware that can directly impact the security of an iOS-powered device. iOS configuation profiles give businesses the capability to install and run applications signed by the provider without the scrutiny of Apple's App Store submission and were initially designed for configuration management, for example, use by MDMs. Once approved, Apple provides the developer a signed certificate for the business to apply to the device, enabling them to install any app they have produced in-house onto the device. However, this feature also allowed end-users to sideload unapproved and often unsecured apps without established OEM protections from third-party stores, increasing the risk of data theft and exploitation on the device as there are limited or no vetting of submitted apps in these third-party stores.

iOS configuration profiles serve a wide range of legitimate scenarios for enterprises that have adopted mobile-managed and unmanaged mobile devices into their ecosystem. For example, MDMs use profiles to enforce configurations in the devices, and 30% of the profiles Zimperium evaluates are? from management tools. But the remaining 70% are installed by users, outside the control and visibility of the enterprise.

Most common end-user installed iOS configuration profiles

Figure 15: Zimperium researched data highlighting the most common end-user installed iOS configuration profiles.

Each iOS configuration profile type exposes the user to a different potential risk. While a profile used to set up a font on the device or to install a printer through Airplay could be considered as a low-risk profile to a user, the installation of a new certificate authority could allow a potential attacker to decrypt all the secured traffic from a specific device while a malicious VPN profile or proxy configuration can redirect all the network traffic on the device to a server controlled by a malicious actor.

A malicious profile would enable system-wide settings and allow untrusted certificates to be installed on the device. From free VPNs to proxy configurations, third-party app stores to root certificates, data can be re-routed and shared in its unencrypted state, or data such as contacts and email credentials shared to malicious parties. There is no way to know where any data from compromised devices is sent or decrypted after a malicious profile is loaded.

Risk distribution of unmanaged iOS configuration profiles

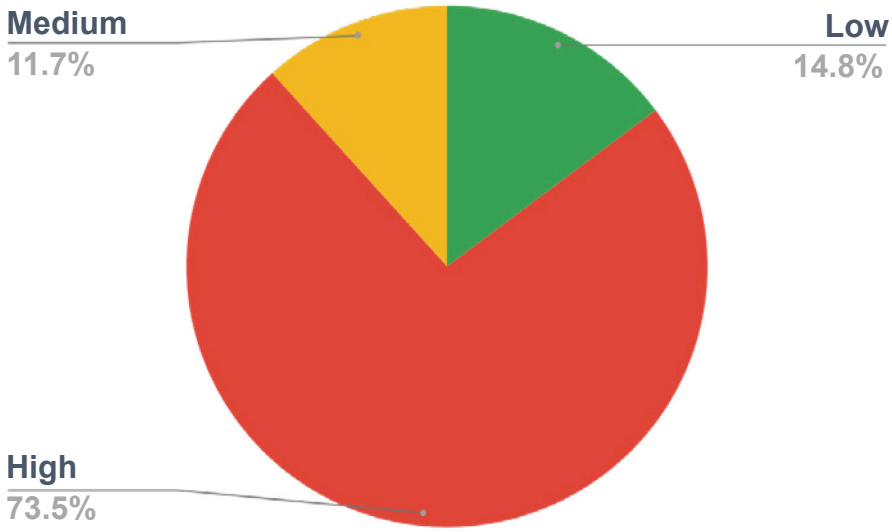


Figure 16: Zimperium researched data highlighting the risk distribution of unmanaged iOS configuration profiles

However, in a report released in October 2021 aiming to defend its locked ecosystem, Apple revealed that this program had inadvertently increased the attack surface of iOS devices with little way to stop the exploitation. A rise in third-party services, like external stores and app signing services, has taken advantage of the feature since its launch to bypass Apple's AppStore security controls, allowing signed applications on non-jailbroken devices.

„Trotz der strengen Kontrollen und des begrenzten Umfangs des Programms haben böswillige Akteure unerlaubte Wege gefunden, um darauf zuzugreifen, zum Beispiel durch den Kauf von Unternehmenszertifikaten auf dem Schwarzmarkt ... Apple hat seine Bemühungen verstärkt, die Kontrollen des Programms zu verschärfen und den Schutz der Benutzer zu erhöhen, aber der Missbrauch hält an.“[52]

„Trotz der strengen Kontrollen und des begrenzten Umfangs des Programms haben böswillige Akteure unerlaubte Wege gefunden, um darauf zuzugreifen, zum Beispiel durch den Kauf von Unternehmenszertifikaten auf dem Schwarzmarkt ... Apple hat seine Bemühungen verstärkt, die Kontrollen des Programms zu verschärfen und den Schutz der Benutzer zu erhöhen, aber der Missbrauch hält an.“[52]

Ein kompromittiertes Zertifikat ermöglicht systemweite Einstellungen und erlaubt die Installation weiterer signierter Zertifikate oder anderer Anwendungen. Von riesigen Social-Media-Unternehmen bis hin zur Verbreitung von Malware gibt es viele Beispiele für diesen Zertifikatsmissbrauch. Leider entdecken die Unternehmen den Missbrauch erst, wenn das Zertifikat widerrufen wird. Diese vom Benutzer aktivierte Option stellt ein erhebliches Risiko für Unternehmen dar.

Diese Zertifikate ändern die Systemkonfiguration, um effektiv zu sein, aber vergangene Angriffe haben gezeigt, wie viele Daten durch diesen Missbrauch abgerufen, freigegeben und verändert werden können. Ein kompromittiertes Zertifikat würde systemweite Einstellungsänderungen und die Installation zusätzlicher signierter Zertifikate für andere, nicht zugelassene Anwendungen ermöglichen. Von kostenlosen VPNs über Proxy-Konfigurationen und App-Stores von Drittanbietern bis hin zu Root-Zertifikaten können Daten umgeleitet und in unverschlüsseltem Zustand weitergegeben oder Daten wie Kontakte und E-Mail-Anmeldedaten an böswillige Parteien weitergegeben werden. Es gibt keine Möglichkeit herauszufinden, wohin die Daten von einem kompromittierten Gerät gesendet werden oder welche Daten entschlüsselt werden, nachdem ein schädliches Profil geladen wurde.

Die Zahl der Zero-Day-Exploits gegen Apples iOS-Geräte stieg im Jahr 2021 mit 11 Zero-Day-Schwachstellen, die in freier Wildbahn entdeckt wurden. Obwohl Malware, die gegen iOS-Geräte eingesetzt wird, nicht so häufig in den Nachrichten auftaucht, erhalten die Bugs und Schwachstellen aufgrund ihrer Auswirkungen und ihres Kundenstamms große Aufmerksamkeit.

Im Jahr 2021 wurden 11 verschiedene Zero-Day-Exploits für Apple iOS und Apple WebKit aufgedeckt, was 19 % aller Zero-Day-Exploits in diesem Jahr ausmacht. Der Sicherheitsanbieter ZecOps enthüllte außerdem die Forschungsergebnisse zu WiFiDemon, einer Zero-Click-Wi-Fi-Proximity-Schwachstelle in iOS 14 bis iOS 14.4 ohne zugewiesene CVE[53] Das Forschungsteam von ZecOps berichtet, dass es sich bei dem Netzwerkabsturz eigentlich um eine nicht gepatchte Zero-Day-Schwachstelle handelte. Die Sicherheitslücke ermöglichte es Angreifern, aus der Ferne Code auf dem Telefon oder Tablet des Opfers auszuführen, ohne dass der Endbenutzer eingreifen konnte oder benachrichtigt wurde. Während die Zero-Click-Komponente der Sicherheitslücke mit iOS 14.4 gepatcht wurde, erhielten neuere Versionen des mobilen Betriebssystems den Patch erst mit der Veröffentlichung von iOS 14.7.

Mehr Apps bedeutet eine Gefährdung für mehr als nur Daten

Für Entwickler von mobilen Anwendungen ist es eine Sache, eine unglaubliche, einzigartige Idee für eine mobile Anwendung zu haben. Doch was ist mit der Sicherheit? Die Sicherheit einer mobilen Anwendung ist von entscheidender Bedeutung, zumal sich die Angriffe auf mobile Geräte ständig weiterentwickeln und ausweiten. Mobiltelefone und Apps sind ein weiches Ziel – eine Tatsache, der sich Angreifer sehr bewusst sind.

Im ersten Quartal 2021 waren fast 3,5 Millionen Apps im Google Play Store und 2,2 Millionen Apps im Apple App Store verfügbar.[54]

Zimperium analysiert Schwachstellen, Malware und das Gesamtrisiko von Millionen von Anwendungen. **Unsere Ergebnisse zeigen, dass es 41 % der iOS-Apps an einem soliden Datenschutz mangelt, während 26 % der Android-Apps mit demselben Problem zu kämpfen haben.** Die Einführung von Verschlüsselung ist unzureichend, da schlechte Implementierungen und Schlüsselverwaltungspraktiken dazu führen können, dass vertrauliche und kryptografische Daten für Unbefugte zugänglich werden.

Wir haben festgestellt, dass 40 % der Android-Apps und 52 % der iOS-Anwendungen mindestens einen anfälligen Verschlüsselungsalgorithmus verwenden. Darüber hinaus wiesen 81 % der Android-Apps einen unzureichenden Code-Schutz auf, bei iOS waren es nur 72 %.

Die Sicherung einer Anwendung hört nicht mit deren Veröffentlichung auf. Durch Reverse-Engineering-Taktiken können Angreifer Schwachstellen im Code der Anwendung finden. Daher ist es von entscheidender Bedeutung, regelmäßig Penetrationstests von Anwendungen durchzuführen. Allerdings geben nur 49 % der Befragten an, dass sie diese Tests für ihre mobilen Anwendungen durchführen.[55]

Die Ergebnisse von Zimperium zeigen auch, dass **75 % der iOS-Apps die Reverse-Engineering-Anforderungen des Open Web Application Security Project (OWASP) Mobile 10-M9 nicht erfüllen, während 24 % der Android-Apps ebenfalls durchfallen.** Auf die Frage, was das größte Risiko für mobile Anwendungen darstellt, gaben 49 % der Befragten an, dass ihre Anwendungen rückentwickelt werden.[56]

Datenschutz und Sicherheit haben für Verbraucher und Unternehmen oberste Priorität, daher ist es von entscheidender Bedeutung, dass Entwickler ihre mobilen Anwendungen schützen. Warum ist dies für Unternehmen so bedeutsam? Immerhin 51 % der Befragten gaben an, dass sie vier bis acht arbeitsbezogene Apps auf ihren mobilen Geräten installiert haben, während 31 % mindestens eine solche App nutzen.[57]

Werden Schwachstellen in mobilen Anwendungen nicht behoben, können sie verheerende Auswirkungen auf den Umsatz, den Ruf der Marke und den alltäglichen Geschäftsbetrieb haben. Die mobile Bedrohungslandschaft entwickelt sich ständig weiter, da neue Schwachstellen und Techniken entdeckt werden. Dies erfordert Sicherheitslösungen, die nicht nur umfassend, sondern auch schnell und einfach zu aktualisieren sind.

In einer kürzlich durchgeführten Umfrage gaben jedoch 49 % der Befragten an, dass sie ihre Anwendungen erst zum Zeitpunkt der nächsten geplanten Veröffentlichung aktualisieren, wenn ein neues Risiko entdeckt wird.[58] Und selbst nach der Veröffentlichung einer neuen Version kann es vorkommen, dass die Kunden diese Aktualisierungen nicht sofort installieren. Insbesondere für Unternehmen mit großen Anwendungen kann dies bedeuten, dass Anwendungen und Daten 12 bis 18 Monate lang ungeschützt bleiben, bis die gesamte Installationsbasis sich für ein Upgrade der Anwendung entscheidet.

	% der Android-	% der iOS-
Apps verfügen über unzureichende Datenschutzmaßnahmen	26 %	41 %
Systeme verfügen über verwundbare Verschlüsselung	40 %	52 %
Apps verfügen über unzureichenden Codeschutz	81 %	72 %

Risiken im Bereich der Mobilanwendungen nach Branchen

Wie bereits erwähnt, besteht eine häufige Schwachstelle darin, dass die Informationen der Endnutzer offengelegt werden. Da kriminelle Akteure weiterhin mobile Anwendungen ausnutzen, sind in mehreren Branchen Compliance- und Regulierungsfaktoren im Spiel:

- **Gesundheitswesen.** Wenn Gesundheitsdaten in die falschen Hände geraten, müssen Organisationen des Gesundheitswesens mit Geldbußen und Strafen nach dem „Health Insurance Portability and Accountability Act“ (HIPAA) rechnen.
- **Finanzdienstleistungen.** Finanzunternehmen müssen bei Datenschutzverletzungen und Verstößen gegen die Vorschriften mit Geldbußen rechnen. Außerdem sind die Sicherheitsverletzungen seit der COVID-19-Pandemie sprunghaft angestiegen.[59]
- **Einzelhandel.** Schlechte Sicherheitspraktiken können dazu führen, dass Einzelhändler bei Verstößen gegen den „Payment Card Industry Data Security Standard“ (PCI DSS) mit Geldstrafen belegt werden. Diese Unternehmen könnten auch mit Gerichtsgebühren und Strafen konfrontiert werden, wenn Verbraucher von einem Cyberangriff betroffen sind.

Unternehmen aller Branchen müssen die einschlägigen regionalen Datenschutzbestimmungen einhalten, darunter die Allgemeine EU-Datenschutzgrundverordnung (GDPR) und den „California Consumer Privacy Act“ (CCPA). Diese Gesetze geben den Verbrauchern bestimmte Rechte in Bezug auf die Verwaltung und Verwendung ihrer Daten. Darüber hinaus gelten sie für alle Organisationen, die personenbezogene Daten von Personen in Regionen verwalten, die unter diese Gesetze fallen. Daher gelten diese Regeln für Finanz-, Einzelhandels- und Gesundheits-Apps sowie für Lifestyle-Apps. Die Nichteinhaltung der Vorschriften kann dazu führen, dass ein Unternehmen mit Geldstrafen und Sammelklagen belegt wird. Dies gilt auch für Fälle, in denen Kundendaten aufgrund unzureichender Sicherheitsmaßnahmen Teil einer Datenschutzverletzung oder eines Cyberangriffs sind.

	Android	iOS
Finanz-Apps		
Mangelnder Datenschutz	**49.9 %**	**41.2 %**
Nutzung verwundbarer Verschlüsselung Algorithmen	**79.8 %**	**42.3 %**
Mangelnder Codeschutz	**64.4 %**	**71.9 %**
Apps für das Gesundheitswesen		
Mangelnder Datenschutz	**45.4 %**	**36.6 %**
Nutzung verwundbarer Verschlüsselung Algorithmen	**72.4 %**	**41.4 %**
Mangelnder Codeschutz	**82.4 %**	**72.2 %**
Retail Apps		
Mangelnder Datenschutz	**61.1 %**	**48.0 %**
Nutzung verwundbarer Verschlüsselung Algorithmen	**80.4 %**	**54.0 %**
Mangelnder Codeschutz	**69.7 %**	**82.34 %**
Lifestyle Apps		
Mangelnder Datenschutz	**54.6 %**	**44.5 %**
Nutzung verwundbarer Verschlüsselung Algorithmen	**77.4 %**	**49.0 %**
Mangelnder Codeschutz	**74.8 %**	**74.0 %**

Die Risiken, die von „undichtem“ Cloud-Speicher ausgehen

Viele Apps verlassen sich für ihre Funktionen auf Cloud-Speicher. Entwickler können die Cloud zur Speicherung von Konfigurationsdateien, Mediendateien und anderen Ressourcen nutzen. Den Cloud-Speicher für eine App einzurichten ist unglaublich einfach. Die Einrichtung der dringend benötigten Sicherheitskonfiguration wird jedoch meist leider nicht priorisiert oder völlig übersehen. Dies bringt erhebliche Risiken mit sich: Durch die Analyse von Apps können Angreifer feststellen, of eine App Cloud-Speicher nutzt und, was noch wichtiger ist, ob dieser Cloud-Speicher durch Sicherheitsmaßnahmen geschützt ist.

Es sei darauf hingewiesen, dass Entwickler in einigen Fällen mit Beispielcode oder Bibliotheken arbeiten, die auf Cloud-Speicher zugreifen, und sich dieser Abhängigkeiten nicht einmal bewusst sind. Infolgedessen kennen sie möglicherweise die potenziellen Risiken nicht, geschweige denn, dass sie sich mit ihnen auseinandersetzen konnten.

Durch den Zugriff auf den Cloud-Speicher kann ein Angreifer sensible Informationen wie Gesundheitsdaten, Konfigurationsdateien, personenbezogene Daten und vieles mehr auslesen. In mindestens einem Fall war ein Angreifer in der Lage, die Kontrolle über die gesamte Cloud-Infrastruktur eines App-Entwicklers zu übernehmen.

	Android	iOS
%	**18.85 %**	**8.19 %**
Gesamtzahl der analysierten Apps (seit Januar 2020)	**232.760**	**325.200**
Gesamtzahl der Anwendungen mit unsicherer Cloud-Konfiguration	**43.892**	**26.639**

Warum MTD für XDR so wichtig ist (SentinelOne)

Rick Bosworth, Director of Product Marketing, SentinelOne

7 von 10

Unternehmen geben an, dass Mobiltelefone für ihr Unternehmen von entscheidender Bedeutung sind

1 von 3

Zero-Day-Angriffen auf iOS- und Android-Geräte abzielte

Mobile Geräte sind zu einer schützenswerten Kategorie geworden. Telearbeitsplätze und BYOD-Richtlinien sind heute die Regel, nicht die Ausnahme **und 7 von 10 Unternehmen geben an, dass Mobiltelefone für ihr Unternehmen von entscheidender Bedeutung sind[60].** Derselbe Anteil der Mitarbeiter verwendet seine persönlichen Mobilgeräte, um auf Unternehmensressourcen zuzugreifen – Kundenlisten, Kontostrategien, Finanzmodelle und so weiter. Ironischerweise sind mobile Geräte das primäre Mittel (z. B. über eine 2FA-App) zur Überprüfung der Identität und des gegenseitigen Vertrauens beim Zugriff auf diese Ressourcen. Und das macht sie zu einem Hauptziel in der Angriffsfläche Ihres Unternehmens, was verdeutlicht, **warum die Abwehr mobiler Bedrohungen eine wichtige Komponente eines XDR-Sicherheitssystems ist.**

Es ist ein weit verbreiteter Irrglaube, dass mobile Betriebssysteme von Haus aus sicher sind. Obwohl Sicherheitsfachleute wissen, dass dies falsch ist, müssen sie dennoch ein skeptisches Management – Sie wissen schon, diejenigen, die den Finanzrahmen bestimmen – von der Notwendigkeit überzeugen. Zero-Day-Exploits, bösartige Anwendungen, riskantes Benutzerverhalten und Phishing-Angriffe sind sehr reale Bedrohungen für das mobile Unternehmen. Google Project Zero berichtet, dass im Jahr 2021 **einer von drei Zero-Day-Angriffen auf iOS- und Android-Geräte abzielte;** im Jahr zuvor war es noch einer von zehn. In die App-Stores werden bösartige Apps hochgeladen, welche die Sicherheitskontrollen umgehen; eine bösartige 2FA-App wurde im Februar 2022 aus dem Google Play Store entfernt, nachdem sie 10 000 Mal heruntergeladen worden wa[61]. Die Nutzer jailbreaken ihre Geräte und laden Apps per Sideload. Betrügerische Zugangspunkte in stark frequentierten Bereichen wie Cafés fangen den Datenverkehr ab. Und dann ist da natürlich noch das allgegenwärtige Gespenst der Phishing- (E-Mail) und Smishing-Angriffe (SMS).

Mobile Threat Defense (MTD) widmet sich speziell der Prävention, Erkennung und Reaktion auf Bedrohungen für mobile Geräte, die iOS, Android und sogar Chrome OS nutzen. Die meisten Unternehmen verfügen bereits über ein System zur Verwaltung mobiler Geräte (MDM), aber MDM bedeutet nicht Sicherheit. Es handelt sich um Management: Verwaltung und grundlegende Umsetzung. Ein MDM als Sicherheitslösung zu bezeichnen, ist so, als würde man einen Handwerker als Klempner bezeichnen: Sicher, es gibt ein paar Überschneidungen, aber Sie wissen, wen Sie anrufen müssen, wenn ein Frostschaden Ihre Rohre zum Platzen bringt. Ein MDM eignet sich hervorragend für die Verwaltung: ein Smartphone verfolgen, sperren, löschen. Im Gegensatz dazu schützt MTD ein Unternehmen vor Phishing-Angriffen, Malware und Netzwerk-Exploits wie Man-in-the-Middle-Angriffen. MTD und MDM sind komplementäre Lösungen und schließen sich nicht gegenseitig aus.

Die Sicherung mobiler Geräte ist ein wichtiger Aspekt jeder XDR-Strategie

Mobile Geräte sind nur eine von vielen Angriffsflächen - Benutzerendgeräte, Cloud-Workloads, IoT, E-Mail, Identität und so weiter. Das Wesen von XDR ist ein dreistufiger, maschinenschneller Prozess: (1) Aufnahme von Daten aus diesen vielfältigen Angriffsflächen, (2) Automatisierung der Analyse und Korrelation, Gewinnung von Erkenntnissen und (3) Vorschreiben und möglicherweise Automatisieren von Reaktionsmaßnahmen auf der Grundlage der gewonnenen Erkenntnisse. Es gibt einige gute Gründe, eine MTD-Lösung in Ihr Sicherheitssystem einzubinden. **Allein die Erkennung eines Angriffs auf einen mobilen Benutzer, selbst wenn dieser erfolgreich von einer MTD-Lösung blockiert wird, kann sich für das Sicherheitsmanagement (SOC) als aussagekräftige, verwertbare Information erweisen.**

Nehmen wir das Beispiel einer hochrangigen Zielperson, vielleicht ein CEO, der zum Flughafen gefahren wird. Sie nimmt Anrufe entgegen und liest E-Mails, von denen eine von einem Abteilungsleiter stammt und welche einen Link zu Informationen enthält, die ihre Aufmerksamkeit erfordern. Natürlich handelt es sich um einen sorgfältig ausgeklügelten Spear-Phishing-Angriff. Mit einer MTD-Lösung wird der Angriff auf ihr Mobiltelefon sofort durch verhaltensbasierte KI erkannt, gestoppt und das SOC alarmiert. Mit der Cross-Stack-Transparenz wird der Angriff sofort auf einen erfolgreichen Phish der E-Mail des Bereichsleiters zurückgeführt. In einer XDR-Welt führt diese Bestätigung automatisch zu einer Rücksetzung der E-Mail-Anmeldedaten. Die Sicherheitsabteilung ruft dann den CEO an, um ihr zu versichern, dass sie nicht nur sicher ist, sondern dass man auch die Ursache gefunden hat und die Situation im Griff hat, und das alles innerhalb von 2 Minuten... oder weniger. Im Gesamtbild wird das SOC auf eine aktive Kampagne aufmerksam gemacht, die auf hochrangige Führungskräfte abzielt.

Wenn wir wissen, dass ein mobiles Gerät mit Malware infiziert ist, können wir den Zugang sperren, und das Sicherheitsmanagement kann auch etwas über die Sicherheitskompetenz der Benutzer erfahren.

Ein geeignetes XDR-Modell weist diesem Benutzer automatisch ein Risikoprofil zu und kann sogar ein verknüpftes Berechtigungstool verwenden, um den Zugriff so weit wie möglich einzuschränken und so das Risiko für das Unternehmen zu begrenzen. Oder es kann dem Benutzer häufigere 2FAs aufzwingen, bis das Risiko nachlässt, z. B. durch das Entfernen der bösartigen Anwendung.

Die Funktionsweise von Unternehmen hat sich grundlegend verändert, beschleunigt durch die Ereignisse der letzten zwei Jahre. **Angesichts der Tatsache, dass so viele Mitarbeiter außerhalb der Unternehmensgrenzen tätig sind, entwickeln sich unsere Sicherheitsstrategien weiter, um der Herausforderung gerecht zu werden, unsere Daten sowohl verfügbar als auch vertraulich zu halten. Die Abwehr mobiler Bedrohungen ist entscheidend für den Erfolg unserer zusammenhängenden, plattformübergreifenden XDR-Sicherheitslösung.**

Etablierung von „Mobile Device Trust“ in „Zero Trust“ -Sicherheitsarchitekturen

Loren Russon, Vice President of Product Management, Ping Identity

Die pandemiebedingte Verlagerung von Mitarbeitern in virtuelle, mobile Arbeitsumgebungen hat große Unternehmen dazu veranlasst, sich von herkömmlichen, statischen, perimeterbasierten Sicherheitsansätzen zu lösen. Dieser Wandel macht es für Unternehmen noch dringlicher, in identitätsbasierte Sicherheitsfunktionen als Teil einer Strategie zur Implementierung von Zero-Trust-Sicherheitsmodellen für ihre räumlich verteilten Arbeitskräfte zu investieren.

Das Zero-Trust-Sicherheitsmodell – basierend auf dem Prinzip ***„Niemals vertrauen, immer prüfen“*** – behandelt jeden als potentielle Bedrohung und verhindert einen Datenzugriff, bis eine Verifizierung stattgefunden hat. Die Zero-Trust-Transformation verspricht, neue Herausforderungen zu meistern, um Mitarbeiter, Kunden und Unternehmen vor den sich ständig weiterentwickelnden Cyber-Bedrohungen zu schützen und gleichzeitig die Richtlinieneinhaltung und Mitarbeiterproduktivität zu verbessern. Das Ziel ist es, Mitarbeitern und Kunden ein hervorragendes Online-Erlebnis zu bieten, unabhängig davon, wo die Arbeit erledigt wird.

Angesichts der rasanten Verbreitung mobiler Geräte, die auf Unternehmensressourcen zugreifen, benötigen Sicherheitsteams jedoch bessere Möglichkeiten, um eine vertrauenswürdige Beziehung zu den Geräten im Netzwerk aufzubauen. Um zu gewährleisten, dass Mitarbeiter auf den Geräten, die sie am häufigsten benutzen, sicheren Zugriff auf die benötigten Daten haben, muss Zero Trust mit fortschrittlichem Schutz vor mobilen Bedrohungen aktiviert werden.

Das ist der Punkt, an dem sich die Partnerschaft zwischen Ping Identity und Zimperium auszeichnet. Unsere beiden Unternehmen arbeiten eng zusammen, um Zero-Trust-Sicherheitsmodelle zu verbessern, indem sie umfassende Daten zur mobilen Risikolage liefern. Die Sicherheitslösung von Ping Identity/Zimperium ermöglicht es großen Unternehmen, vertrauenswürdigere Verbindungen zu allen Elementen im Netzwerk herzustellen: Benutzer, Geräte, Anwendungen, Transaktionen, APIs usw.

Aufbau vertrauenswürdiger Verbindungen

Identität ist der entscheidende erste Schritt zum Aufbau einer Zero-Trust-Architektur, denn man kann nur dem vertrauen, was man auch identifizieren kann. Die Identitätssicherheit basiert auf der Idee, dass alle Benutzer und Geräte zunächst authentifiziert werden müssen, bevor sie Zugang zu sensiblen Ressourcen oder Daten erhalten können. Dies mag in der heutigen Zeit selbstverständlich erscheinen, stellt jedoch eine Abkehr von den Sicherheitsansätzen der Vergangenheit dar, bei denen den Benutzern vertraut wurde, sobald sie sich im Unternehmensnetz befanden.

Ping Identity bietet die identitätsbasierte Plattform und die zugrundeliegende Service-Suite, mit der Sicherheitsteams robustere Sicherheitskontrollen und -richtlinien für praktisch jeden Benutzer, jedes Gerät oder jedes andere Element im Netzwerk implementieren können, unabhängig davon, ob die Elemente in einer Cloud-, Hybrid- oder On-Premise-Umgebung arbeiten.

Die Benutzer müssen zum Beispiel auf intelligente Weise authentifiziert werden. Sie müssen ihre Identität mit mehreren Elementen nachweisen, auch bekannt als Multi-Faktor-Authentifizierung (MFA). Die Kombination der Faktoren besteht oft aus einem Nachweis, den der Nutzer kennt, z. B. einem Passwort, einem Gerät, das er besitzt, etwa einem Smartphone, und vielleicht einem biometrischen Faktor wie der Gesichtserkennung oder dem Fingerabdruck. Unterschiedliche Aktivitäten und Sicherheitsrisiken können den Einsatz unterschiedlicher Stufen der Multi-Faktor-Authentifizierung erfordern.

Sich allein auf die Authentifizierung von Nutzern zu verlassen, reicht nicht aus, um eine Zero-Trust-Infrastruktur zu erreichen. Selbst ordnungsgemäß authentifizierte Benutzer können Opfer der Nutzung kompromittierter Mobilgeräte werden. Die Authentifizierung dieser Endgeräte ist für eine wirksame Abwehr von mobilen Bedrohungen ebenso wichtig, da kompromittierte Geräte von Bedrohungen wie Ransomware, Spyware und Trojanern ausgenutzt werden können.

Die Sicherheit mobiler Geräte wird jedoch oft der Bequemlichkeit geopfert. Infolgedessen sind diese mobilen Endgeräte vermehrt Angriffsvektoren ausgesetzt, die für Unternehmen nicht sichtbar sind, geschweige denn verhindert werden können, wodurch Lücken in ihrer Zero-Trust-Architektur entstehen. Und selbst wenn ein mobiles Gerät nachweislich nicht manipuliert wurde, kann es sein, dass ein Sicherheits-Patch fehlt, wodurch die Sicherheitslage eines Unternehmens gefährdet werden könnte.

Zimperium und Ping Identity arbeiten zusammen, um das Identitätsmanagement für mobile Geräte und die Zugriffskontrolle zu verbessern sowie alle mobilen Endgeräte in einen Sicherheitsperimeter einzubinden. Zimperium bietet KI-basierten Echtzeitschutz direkt auf dem Gerät gegen Bedrohungen für Android, iOS und Chromebooks. Diese Echtzeitdaten wiederum erweitern die „Ping Identity“-Plattform um eine größere Sicherheitstransparenz, Zugriffskontrolle und Gerätesicherheit, die für die Absicherung sowohl unternehmenseigener als auch mobiler Endgeräte erforderlich sind. Sicherheitsteams können sich ein besseres Bild von der gesamten Risikolage machen und ihren Schutz vor Angriffen auf Geräte, Netzwerke, Phishing und bösartige Anwendungen verbessern.

Die Technologie überwacht Geräte kontinuierlich und liefert klare, umsetzbare Warnungen, die Sicherheitsteams anweisen, wie sie Sicherheits- oder Compliance-Probleme lösen können. Mit der Echtzeit-Erkennung, -Benachrichtigung und -Reaktion auf mobile Bedrohungen von Zimperium können Sicherheitsteams, welche die „Ping Identity“-Plattform nutzen, sicherstellen, dass die Abdeckung mobiler Endgeräte ein integraler Bestandteil ihrer Zero-Trust-Sicherheitsstrategie ist.

Identität ist die neue Grenze, die Unternehmen absichern müssen, und der beste Weg, dies effektiv zu tun, ist die Nutzung eines Zero-Trust-Ansatzes, der die Abwehr mobiler Bedrohungen mit starker Authentifizierung vereint.

Die Integration der IAM-Plattform von Ping Identity mit Zimperium erleichtert den Sicherheitsteams die Implementierung von Zero-Trust, um eine nahtlose und sichere Benutzererfahrung zu gewährleisten.

Die bereits große und weiter wachsende Angriffsfläche von Smartphones

Julian Durand, VP Product Management, Intertrust

Die Zahl der mit dem Internet verbundenen Smartphones ist rasant gestiegen. Da sie für unser privates und berufliches Leben immer wichtiger werden, sind ihre Technologie und Anwendungen komplexer und vernetzter geworden und damit auch ein größeres Ziel für böswillige Akteure. Um uns jedoch bestmöglich auf die Bedrohungen von heute und morgen vorzubereiten, müssen wir die Angriffsfläche für mobile Smartphones verstehen und die drei wichtigen Ebenen der Erkennung, des Schutzes und der Verteidigung untersuchen, um die Risiken der Angriffsfläche zu minimieren.

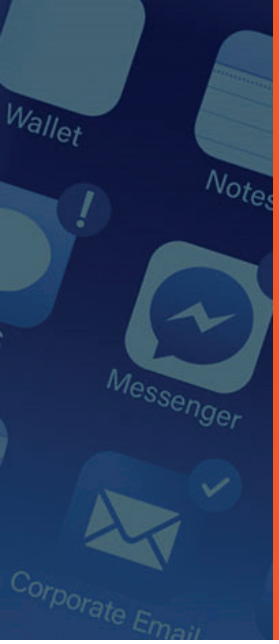
Die weltweiten jährlichen Smartphone-Lieferungen sind von 173,5 Millionen im Jahr 2009 auf 1,43 Milliarden im Jahr 2022 gestiegen, was einer durchschnittlichen jährlichen Wachstumsrate von über 10 % in 23 Jahren entspricht[62]. Sie wäre sogar noch höher, wenn die Halbleiter-Lieferketten nicht von der Pandemie beeinträchtigt worden wären.

Heute übersteigt die Zahl der mit dem Internet verbundenen Mobiltelefone leicht die Weltbevölkerung von 7,6 Milliarden.

Auch wenn die Dichte variiert, von sehr hoch auf den Malediven (246 Mobilfunkanschlüsse pro 100 Einwohner) bis zu sehr niedrigen Werten wie in Kuba und Nordkorea (12 Anschlüsse pro 100 Einwohner), ist es doch eine Tatsache, dass Mobiltelefone inzwischen allgegenwärtig sind[63].

Um die Bedrohungen für die Cybersicherheit dieser allgegenwärtigen Geräte besser zu verstehen, bietet das U.S. National Institute of Standards and Technology (NIST) einen Katalog für mobile Bedrohungen an[64]. Hierbei handelt sich um einen nützlichen Rahmen, um das Wachstum der Angriffsfläche dieser Systeme aufzuzeigen, vor allem wenn man sie durch die Linse der Identifizierung und Abschwächung von Unternehmens-Cyberrisiken betrachtet. Wie wir sehen werden, ist die Angriffsfläche nicht linear, sondern vielleicht sogar exponentiell gewachsen, da jedes Komplexitätselement, die Anzahl der Verbindungen und die zentrale Bedeutung dieser Geräte für unser Leben ein solch dramatisches Wachstum aufweisen. Zusammengenommen stellen diese Faktoren ein komplexes Wachstum dar, da jedes Element die nächste Bedrohungsstufe verschärft und die gesamte Angriffsfläche im Zusammenhang mit der Unternehmenskommunikation weiter vergrößert.

Der Technologie-Stack eines Smartphones beginnt heute mit den Chips, welche die Anwendungs- und Kommunikationsleistung bereitstellen. Das Flaggschiff Snapdragon 8 Gen1 von Qualcomm gibt beispielsweise einen Eindruck davon, was 2022 in Smartphones zu finden sein wird. Dazu gehören eine 3-GHz-Multicore-CPU, eine leistungsstarke KI-Engine, ein mit 10 Gbit/s getaktetes 5G-Modem, eine Spiele-Engine der Konsolenklasse, ein fortschrittliches Ortungsmodul, das sechs separate GNSS-Satellitensysteme (Global Navigation Satellite System) mit mehreren Konstellationen unterstützt, fortschrittliche Kamera-, Video- und Sensorverarbeitungsmodule sowie die neuesten Wi-Fi-, Bluetooth- und NFC-Modems - alles in einem 4-nm-Prozessknoten[65].



All diese Hardware erfordert Firmware für den Zugriff auf den Einschalt-Selbsttest, den anfänglichen Bootloader und Treiber für jeden dieser Technologiekerne.

Ein mobiles Betriebssystem wie iOS oder Android baut weiter auf der Firmware auf. Android, das weltweit beliebteste Betriebssystem für Mobiltelefone, hat kürzlich seine 11. Version veröffentlicht. Die Aktualisierung eines Smartphones erfordert einen Download von etwa 2 GB[66]. Das ist eine Menge Software mit einer beliebigen Anzahl neuer Funktionen, von denen jede eine erhebliche Komplikation und potenzielle Möglichkeiten für mehrere neue Bedrohungen darstellt. Allein die Größe des Betriebssystems trägt erheblich zu der schnell wachsenden Angriffsfläche bei, die mit mobilen Geräten verbunden ist.

Und was wäre ein Smartphone heute ohne App-Downloads?

Apps bieten eine noch breitere und viel heterogenere Quelle von Bedrohungen, da sie mit Malware, Schwachstellen für Malware oder oft mit beidem belastet sein können.

Ein modernes Smartphone bietet heute eine Vielzahl von Verbindungsmöglichkeiten, von denen jede einem Eindringling eine direkte Angriffsmöglichkeit bieten kann. Dazu gehören:

- Ein Mobilfunkmodem, das sich automatisch mit dem Mobilfunkmast mit dem besten Signal verbindet. Betrügerische Stationen können auf ein Zielgerät eingestellt und fokussiert werden, um den Eindruck zu erwecken, dass es sich um die Station handelt, mit der sich das Telefon verbinden sollte.

- Bluetooth ist wegen seiner Sicherheitsmängel vielfach kritisiert worden. Zu den Bluetooth-Angriffen gehören:
  - Bluejacking - Senden beliebiger schadhafter Nachrichten an das Telefon einer Person
  - Bluesnarfing - Diebstahl von Informationen
  - Bluebugging - Remotecodeausführung und Geräteübernahme

- Wi-Fi verfügt über mehrere Sicherheitsprotokolle, von denen die meisten unwirksam und fehlerhaft sind. Selbst wenn die Netzwerkebene gesichert ist, verbindet sich ein Smartphone an öffentlichen Orten wie Cafés, Hotels und Flughäfen oft mit Hotspots zweifelhafter Vertrauenswürdigkeit. Selbst wenn die Verbindung geschützt ist, ist es für einen Hotspot, der von einem bösen Akteur kontrolliert wird, trivial, die Kommunikation auszuspionieren, abzufangen und zu verändern.

Die Zero-Trust-Netzwerkarchitektur (ZTNA) ist ein Ansatz, um unabhängig vom Stand der Netzsicherheit die Integrität und den Schutz der Privatsphäre der Kommunikation zu gewährleisten. Intertrust bietet eine ZTNA-basierte Lösung an, die eine End-to-End-Architektur für mobile Geräte in der Cloud bereitstellt, mit der Unternehmen sensible Daten umfassender schützen können.

Smartphones sind mobile Allzweckcomputer, die mit Apps individualisiert werden. Diese Anwendungen werden von App-Stores heruntergeladen. Wenn Sie also dem App-Store vertrauen, können Sie sich auch auf die von ihm vertriebenen Anwendungen verlassen.

Dies kann bis zum äußersten getrieben werden. Der aktuelle Rechtsstreit zwischen dem größten Spielehersteller der Welt und einem der größten Technologieunternehmen der Welt ist ein Beispiel dafür. Epic Games reichte Klage gegen Apple ein, weil das Unternehmen das Apple-Smartphone-Ökosystem kontrolliert und es den Apple-Nutzern unmöglich macht, einen konkurrierenden App-Store zu nutzen. Epic hat Klage eingereicht, weil sie der Meinung sind, dass Apples 30-prozentige Umsatzbeteiligung für Apps Freemium-Spiele wie Fortnite zu teuer macht. Apple behauptet, es ginge nur um Cybersicherheit, obwohl die Wahrheit viel komplizierter ist. Es zeigt jedoch, dass es unbedingt notwendig ist, dass Anwendungen überprüft und kryptografisch signiert werden, um ihre Integrität und Authentizität zu gewährleisten.

- Unternehmen entwickeln zunehmend ihre eigenen Anwendungen, die sie selbst verifizieren und verschlüsselt signieren, um die Echtheit und Integrität der Anwendungen zu garantieren. Richtig ausgeführt ist dies eine sichere Methode, um den Mitarbeitern eines Unternehmens zusätzliche Funktionen zur Verfügung zu stellen. Bei einer schlechten Umsetzung stellt dies jedoch nur einen weiteren Angriffspunkt dar.

- In jedem Fall stellen die von Unternehmen entwickelten Apps allerdings ein weiteres, schnell wachsendes Element der mobilen Angriffsfläche im Unternehmen dar.

Das Smartphone als IoT-Hub

Da Smartphones mittlerweile allgegenwärtig sind und über signifikante Cybersicherheitsfunktionen verfügen, werden sie häufig für die Verwaltung von IoT-Geräten und -Netzwerken („Internet of Things“ oder auch „Internet der Dinge“) genutzt. Sogar Autos können über das Telefon ein- und ausgeschaltet werden.

Dieser Komfort ist sowohl bei Verbrauchern als auch bei Unternehmen beliebt. Allerdings vergrößert sich dadurch die Angriffsfläche erheblich, da viele IoT-Geräte und -Netzwerke, insbesondere die von Verbrauchern genutzten, nicht über die gleichen ausgefeilten Cybersicherheitsfunktionen verfügen wie moderne Smartphones. So können Angreifer Geräte, Hubs und Gateways übernehmen und darauf warten, dass ein anfälliges Gerät eine Verbindung herstellt. Auf diese Weise verbreitete sich die Malware, die das Mozi-Botnet verbreitete, so schnell auf der ganzen Welt[67].

Malware wie Mozi kann auf der Lauer liegen. Wenn ein Smartphone mit einer Sicherheitslücke eine Verbindung zu einem kompromittierten IoT-Hub herstellt, wird es angegriffen. Wenn das Smartphone nicht aktualisiert wurde oder andere Schutzmaßnahmen ergriffen wurden, kann es durchaus infiziert werden.

Eindämmung von Bedrohungen – die drei Phasen der Gefahrenabwehr

1. Erkennung von Bedrohungen

- Ein Smartphone überwachen
- Algorithmen zur Erkennung durch maschinelles Lernen sind erforderlich, da die von vielen Malware-Entwicklern verwendeten polymorphen Code-Fähigkeiten den Signaturprüfgeräten entgehen iii. Senden von Warnungen, wenn ein Gerät vermutlich angegriffen wird oder bekannte Schwachstellen aufweist

2. Schutz von Smartphones

- Zusätzlich zu den Funktionen zur Erkennung von Bedrohungen sollte das Gerät über weitere automatisierte Cybersicherheitsfunktionen verfügen, z. B. automatisches Herunterladen und Anwenden der neuesten authentifizierten Cybersicherheits-Patches
- Schutz vor Phishing-Nachrichten durch Sandboxing-Techniken
- On-Demand-VPN-Funktionen zum Schutz von Daten vor nicht vertrauenswürdigen Gateways und (insbesondere) Wi-Fi-Routern
- Zugangskontrollen zur Abschottung von sensiblen Informationen und Prozessen
- Für Unternehmen ist es besonders wichtig, die Umsetzung von Richtlinien zu skalieren, um sicher zu sein, dass Cyber-Sicherheitsrisiken angemessen angegangen werden

3. Verteidigung

- Neben der Erkennung und dem Schutz geht es bei der Verteidigung um die Skalierung der Abwehrmaßnahmen eines Unternehmens
- Dies umfasst geräteunabhängige Cybersicherheitssysteme, zentralisierte Websicherheit für Geräte und Server sowie Tools für ein einheitliches Identitäts- und Zugriffsmanagement (IAM, „Identity and Access Management“), Schutz vor Datenverlust (DLP, „Data Loss Prevention“) und Cloudzugang-Sicherheitsvermittler (CASB, „Cloud Access Security Broker“)

Ende-zu-Ende-Datensicherheit

Darüber hinaus ist der Einsatz einer Zero-Trust-Architektur im Netzwerk von entscheidender Bedeutung, insbesondere für Unternehmen und IoT-bezogene Anwendungsfälle, da es viele bedeutende und sehr leistungsfähige, auf das Netzwerk ausgerichtete Angriffstechniken gibt. Verwenden Sie einen Gerät-zu-Cloud-Dienst, um sicherzustellen, dass die Daten sicher sind, während sie Netzwerke durchqueren, unabhängig davon, ob sie vertrauenswürdig sind oder nicht. Dies wiederum bietet eine weitere Verteidigungsschicht, da der Dienst eine Geräteauthentifizierung beinhaltet, die Angriffe verhindert.

Das Wachstum mobiler, hypervernetzter Computer hat dem größten Teil der Weltbevölkerung einen beispiellosen Zugang zu preiswerter Kommunikation, zu Wissen und zu hochentwickelten Computern verschafft. Die große Reichweite und der hohe Entwicklungsstand dieser mobilen Computerplattformen hat uns auch einem Risiko ausgesetzt, insbesondere in Unternehmen, die sensible Daten verwalten. Die Anerkennung dieser Bedrohungslage ist der erste Schritt, und die Entwicklung von Verfahren zur Erkennung, zum Schutz und zur Verteidigung ist wichtiger denn je. Glücklicherweise haben wir die Werkzeuge und das Fachwissen, um sowohl die Angriffsflächen zu reduzieren als auch die Risiken zu minimieren. Aber es braucht Engagement, geeignete Werkzeuge und eine abgestimmte Vorgehensweise, die von der Geschäftsleitung vorangetrieben werden muss.

Die erhöhten Risiken mobiler Produktivitätswerkzeuge für Unternehmen

JT Keating, SVP of Product Strategy, Zimperium

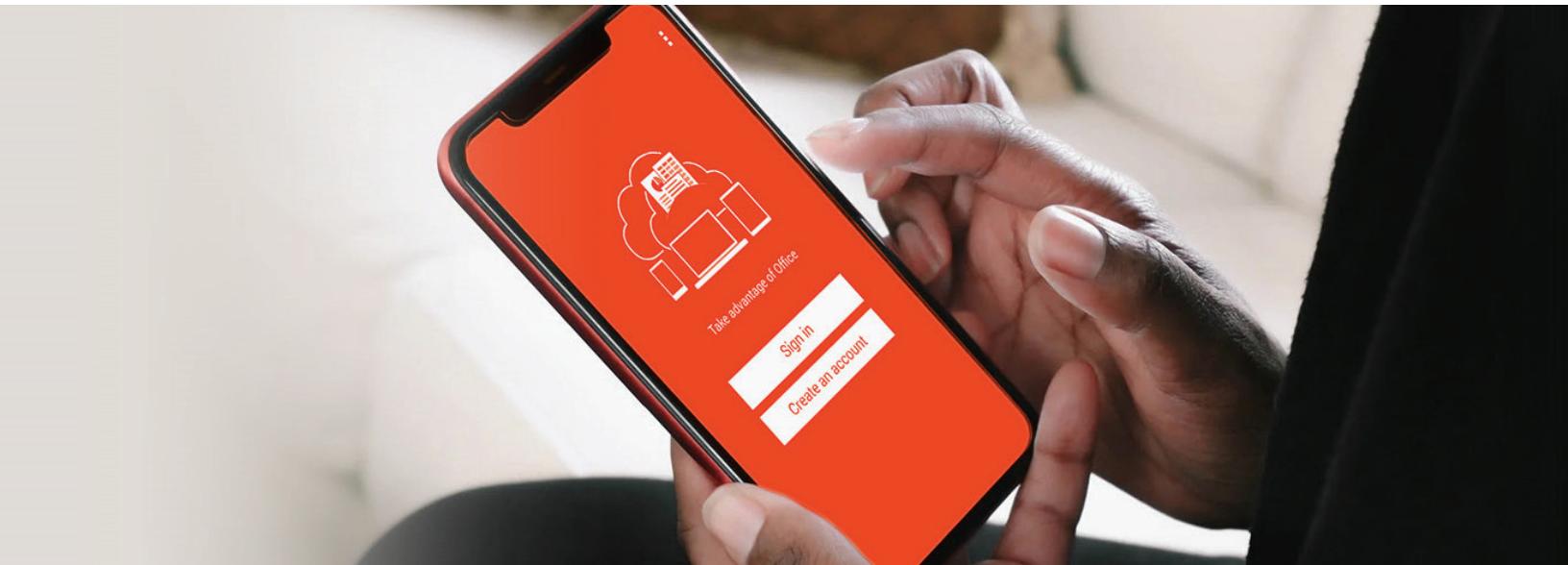
Die COVID-19-Pandemie löste eine Welle von Telearbeitern aus und veränderte die Art und Weise, wie Unternehmen heute arbeiten, erheblich. Zu Beginn des Lockdowns packten die Mitarbeiter schnell Laptops, Monitore und andere Geräte ein, um ihre Arbeit von zu Hause aus fortführen zu können. Während die Arbeit von zu Hause aus vor dem Jahr 2020 als zusätzlicher Vorteil angesehen wurde, ist sie heute für die meisten eine Selbstverständlichkeit. Gleichzeitig nahmen BYOD-Richtlinien und die Erlaubnis der Nutzung von Produktivitäts-Tools auf persönlichen Mobilgeräten durch die Arbeitgeber deutlich zu, um sicherzustellen, dass ihre verteilte Belegschaft die nötigen Werkzeuge und Konnektivität besitzt, um in ihrer neuen Umgebung genauso oder sogar noch produktiver zu sein.

Seitdem haben sich mobile Geräte zu unverzichtbaren Produktivitätswerkzeugen am modernen Arbeitsplatz entwickelt und bieten ihren Nutzern denselben Zugriff auf Anwendungen und Daten, den herkömmliche Endgeräte seit Jahren haben. Tatsächlich gaben 84 % der Sicherheitsexperten, die an einer aktuellen Umfrage von Zimperium teilnahmen, an, dass sie Microsoft Office 365 auf mobilen Geräten aktiviert haben[68].

84 % der Sicherheitsexperten, die an einer aktuellen Umfrage von Zimperium teilnahmen, an, dass sie Microsoft Office 365 auf mobilen Geräten aktiviert haben.

Die Nutzung von Produktivitäts-Tools wie Office 365 ermöglicht den Zugriff auf Office 365-Inhalte wie E-Mails, Teams-Nachrichten, Dokumente und vieles mehr, was die Kommunikation und Zusammenarbeit im Team verbessert. Diese cloudbasierten Produktivitätsanwendungen ermöglichen es den Mitarbeitern, sich endlich vom Schreibtisch zu lösen und auch unterwegs produktiv zu sein. IT-Administratoren nutzen die Mobile Geräteverwaltung (MDM, „Mobile Device Management“), um ein höheres Maß an Kontrolle über Geräte zu haben, die auf Anwendungen wie Word, Excel, PowerPoint, Outlook und OneDrive-Inhalte zugreifen, doch dieser Zugriff ist nicht ohne Risiko.

Wenn das Jahr 2020 etwas bewiesen hat, dann, dass sich Angreifer die COVID-19-Pandemie zunutze machen, und zwar zusätzlich zur Ausweitung der Telearbeitskräfte. Es ist keine Überraschung, dass die Zahl der Sicherheitslücken im Mobilbereich seit der Pandemie um 50 % gestiegen ist. Eine gemeinsame Schwachstelle, über die sich verschiedene Sicherheitsexperten einig sind, ist, dass BYOD seit dem Höhepunkt der Pandemie die Angriffsfläche für Unternehmen aller Größenordnungen vergrößert hat. Als Teams sich bemühten, eine dezentrale Belegschaft einzurichten, mussten einige der Umsetzung einer verteilten Belegschaft Vorrang vor der Sicherung aller BYOD-Geräte, einschließlich ihrer eigenen Endpunkte, einräumen.



36 % der von Zimperium befragten Unternehmen gaben an, dass sie die Implementierung von Sicherheitslösungen zum Schutz von Office 365 auf mobilen Geräten abgeschlossen haben, während 38 % noch dabei sind[69]. Eric Green, ehemaliger globaler Leiter für mobile Sicherheit bei HSBC, kommentiert: **„Da O365 auf dem Handy die gleiche Zugriffstiefe bietet, die früher nur Nutzern auf vollständig gesicherten Desktops oder Laptops zur Verfügung stand, wäre es unverantwortlich, die Daten nicht auch auf mobilen Geräten zu sichern.“**

In der heutigen Bedrohungslage müssen mobile Geräte so ausgestattet sein, dass sie vor dem gesamten Spektrum der Risiken und Angriffe in Bezug auf Geräte, Netzwerke, Phishing und bösartige Apps geschützt sind.

Der Schutz des Unternehmens vor mobilen Angriffen umfasst weit mehr als die Überprüfung der MDM-Konformität oder die übermäßige Einschränkung des Geräts, wodurch Mitarbeiter daran gehindert werden, bestimmte Apps herunterzuladen. Folglich kann eine übermäßige Einschränkung des Geräts durch zusätzliche Verwaltungsrichtlinien im Widerspruch zur Verbesserung der Produktivität stehen.

Um den mobilen Zugriff auf Office 365 zu sichern und gleichzeitig die Benutzerfreundlichkeit zu verbessern, müssen Unternehmen die Sicherheitseinschränkungen mit einer Mobilbedrohungen-Verteidigungslösung (MTD, „Mobile Threat Defense Solution“) verringern. MTDs können Bedrohungen erkennen, Eindringlinge abwehren und die für Zero-Trust- und Conditional-Access-Modelle erforderlichen Funktionen zur Risikobestätigung und Bewertung von Geräten bereitstellen.

Obwohl Unternehmen zwischen MDM und MTD wählen müssen, können sie beide nutzen, um Lücken in der Abdeckung, Datenerfassung und Sicherheit zu schließen. Der Schutz der Privatsphäre ist eine wichtige Komponente bei der Sicherung von zu Arbeitszwecken genutzten privaten Geräten, die dazu beiträgt, dass die Akzeptanz mobiler Sicherheit geringer ist als erwartet, aber die Nutzung von MDM und MTD ermöglicht es dem Unternehmen, die Beschränkungen zu lockern. Die Mitarbeiter zögern, BYOD-Geräte vollständig freizugeben, weil sie Bedenken haben, dass die IT-Teams der Unternehmen Zugriff auf persönliche Daten wie Fotos, Telefonnummern und Nachrichten erhalten könnten.

Es scheint vernünftig, dafür zu sorgen, dass diese Mobilgeräte nicht einfach kompromittiert werden können. Kommt es zu einer Sicherheitsverletzung, können die daraus resultierenden Maßnahmen zur Reaktion auf den Vorfall und zur Wiederherstellung kostspielig sein und erhebliche gesetzliche Strafen nach sich ziehen, wenn personenbezogene Daten offengelegt wurden.

Nur wenige würden dem widersprechen. Heute besteht in der Branche ein breiter Konsens darüber, dass mobile Geräte gesichert werden müssen. Es bleibt jedoch abzuwarten, wie wirksam diese mobilen Abwehrmaßnahmen sind. Sie werden von Cyberkriminellen sondiert und getestet, die mobile Geräte zu Recht als das schwächste Glied in der Sicherheitskette ansehen.

Fazit

Im Jahr 2021 wurde die mobile Angriffsfläche durch komplexe Angriffe und Exploits beeinträchtigt, da die Angreifer die größere Angriffsfläche und die Möglichkeiten, die mobile Endgeräte bieten, ausloteten. Wir wurden Zeuge digitaler Angriffe auf Geräte, die von hochrangigen Regierungsmitgliedern, Wirtschaftsführern, Journalisten und vielen anderen genutzt wurden. Auch weltweit verbreitete Anwendungen wurden von Kriminellen ausgenutzt, um Kundendaten, wichtige Anlegerinformationen und vieles mehr zu enthüllen. Auf dem Weg ins Jahr 2022 werden diese mobilen Exploits und Angriffe weiter zunehmen, da die Abhängigkeit von mobilen Geräten weiter wächst.

Die Neuartigkeit des mobilen Datenzugriffs hat in der Vergangenheit oft den Bedarf an fortschrittlichen Sicherheitsmaßnahmen überschattet, aber das Jahr 2021 hat gezeigt, dass die mobilen Sicherheitsrisiken für Unternehmen, Behörden und Menschen höher sind als je zuvor. Die Techniken und Fähigkeiten der Täter werden immer weiter optimiert, so dass das Vertrauen in mobile Geräte schwindet. Ihre Ziele reichen von Finanzkriminalität bis hin zur Datenexfiltration, wobei sie sich die geringeren Sicherheitsvorkehrungen zunutze machen, die oft auf mobilen Systemen bestehen. Mit jeder neu entdeckten Schwachstelle versuchen die Täter, immer mehr Unternehmen und kritische Systeme mit Hilfe der Exploits anzugreifen.

Für Unternehmen ist es wichtig, die strategische Bedeutung der mobilen Sicherheit rund um die mit ihren kritischen Systemen verbundenen Geräte und Anwendungen nicht aus den Augen zu verlieren. Die Welt der Mobiltelefone wird immer komplexer, da jedes Jahr neue Anwendungen, Funktionen und Möglichkeiten eingeführt werden, aber es ist wichtig zu erkennen, dass die Sicherheit ebenso wie diese Geräte ein sich ständig veränderndes Ziel ist. Es geht darum, die damit verbundenen Risiken und ihre potenziellen Auswirkungen zu verstehen und eine wohlüberlegte Entscheidung mit den richtigen Maßnahmen und Ressourcen zu treffen.

Es ist an der Zeit, dass für mobile Endgeräte und Anwendungen die gleichen Sicherheitserwartungen gelten wie für herkömmliche Geräte. Da die Ökosysteme

Da sich mobile Bedrohungen ständig weiterentwickeln und ausbreiten, werden die branchenführenden Sicherheitstools und -funktionen von Zimperium

It is essential for enterprises not to lose sight of the strategic importance of comprehensive mobile security surrounding the devices and applications connected to their critical systems.

Quellen

1. Zimperium. (2021). When did your organization actively enable BYOD?. Pulse QA
2. Zimperium. (2021). How many work-specific apps are installed on your mobile device?. Pulse QA
3. Zimperium. (2021). Which technology will be your top priority to invest in next year?. Pulse QA
4. IBM. (2021) Cost of a Data Breach Report 2021. https://www.ibm.com/security/data-breach
5. Karta, Y. (2013, January 14). Classifier-based security for computing devices. Google Patents. https://patents.google.com/patent/US9208323B1/en
6. Margaritelli, S. (2018, September 7). Detecting malware in mobile applications via static analysis. Google Patents. https://patents.google.com/patent/US10929532B1/en
7, 15, 20, 29. Zimperium. (2021). Secure Access Practices In North America. Pulse QA
8. Zimperium. (2021). How many work-specific apps are installed on your mobile device?. Pulse QA
9. Zimperium. (2021). When did your organization actively enable BYOD?. Pulse QA
10. Statista. (2021). Number of smartphones sold to end users worldwide from 2007 to 2021. https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/
11, 12, 13. O'Dea, S. (2021, August 4). Smartphones in the U.S. - Statistics & Facts. Statista. https://www.statista.com/topics/2711/us-smartphone-market/#dossierKeyfigures
14. Zimperium. (2021). What's your top endpoint security worry?. Pulse QA
16. Zimperium. (2021). How long does it take your organization to patch impacted endpoints in your enterprise after an emergency or high-priority patch or hotfix that would affect security becomes available?. Pulse QA
17. Zimperium. (2021). How have you shifted your remote work strategy as an organization as a result of cybersecurity incidents in the past year?. Pulse QA
18. Chebyshev, V. (2021, April 28). IT threat evolution Q3 2019. Statistics. Securelist. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/
19. Zimperium. (2021). AI In Cybersecurity. Pulse QA
21. Zimperium. (2021). How would you currently describe your company's cybersecurity strategy?. Pulse QA
22. Zimperium. (2021). Do you agree with this statement? IT teams agree trying to set and enforce corporate policies around cybersecurity is impossible now that the lines between personal and professional lives are so blurred. Pulse QA
23. Zimperium. (2021). Is it right for a company to expect you to use your personal phone number when you work from home? Pulse QA
24. Zimperium. (2021). The majority of smartphone devices in my organization are:. Pulse QA
25. Zimperium. (2021). The majority of tablets in my organization are:. Pulse QA
26. Zimperium. (2021). Which departments/groups within your organization present the biggest risk for insider threats?. Pulse QA
27. Zimperium. (2021). Which of the following areas will receive the greatest investment by the end of the year? Pulse QA
28. Zimperium. (2021). Which of the following category of endpoints represents the weakest security in your organization?. Pulse QA
30. Hunt, S. (2021, December 22). Mobile Security Market 2022. Datamation. https://www.datamation.com/security/mobile-security-market/
31. TechJury. (2022) 55+ Jaw Dropping App Usage Statistics in 2022. Techjury. https://techjury.net/blog/app-usage-statistics/#gref
32. Statista. (2021). Mobile app revenue worldwide 2017–2025, by segment. https://www.statista.com/forecasts/1262892/mobile-app-revenue-worldwide-by-segment
33, 36. Curry, D. (2022, January 11). Mobile Payments App Revenue and Usage Statistics (2022). Business of Apps. https://www.businessofapps.com/data/mobile-payments-app-market/
34. ReportLinker. (2021). Biometric Authentication and Identification Market - A Global and Regional Analysis: Focus on End User, Function, Product Type, Deployment Model and Country - Analysis and Forecast, 2021–2026. https://www.reportlinker.com/p06178590/Biometric-Authentication-and-Identification-Market-A-Global-and-Regional-Analysis-Focus-on-End-User-Function-Product-Type-Deployment-Model-and-Country-Analysis-and-Forecast.html?utm_source=GNW
35. Ericsson. (2018). 5G estimated to reach 1.5 billion subscriptions in 2024 – Ericsson Mobility Report. Telefonaktiebolaget LM Ericsson. https://www.ericsson.com/en/press-releases/2018/11/5g-estimated-to-reach-1.5-billion-subscriptionsin-2024--ericsson-mobility-report
37. FBI. (2021). Internet Crime Complaint Center (IC3) | Cybercriminals Tampering with QR Codes to Steal Victim Funds. https://www.ic3.gov/Media/Y2022/PSA220118
38. Mordor Intelligence. (2021). Global Mobile Cloud Market | 2022 - 27 | Industry Share, Size, Growth - Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/global-mobile-cloud-market-industry
39. Morrison, S. (2019, December 28). His Amazon Ring doorbell got hacked. Now he's suing. Vox. https://www.vox.com/recode/2019/12/27/21039517/amazon-ring-hacking-lawsuit
40. Page, C. (2021, February 11). Slack Urges Users To Reset Passwords After Android Bug Potentially Exposed Credentials. Forbes. https://www.forbes.com/sites/carlypage/2021/02/11/slack-urges-users-to-reset-passwords-after-android-bugpotentially-exposed-credentials/?sh=64d367cf683c
41. Abrams, L. (2021, May 27). Klarna mobile app bug let users log into other customers' accounts. BleepingComputer. https://www.bleepingcomputer.com/news/security/klarna-mobile-app-bug-let-users-log-into-other-customers-accounts/
42. Sharma, M. (2021, May 20). Android apps put data of 100 million Google Play Store users at risk. TechRadar. https://www.techradar.com/uk/news/android-apps-put-data-of-100-million-google-play-store-users-at-risk
43. Newman, L. H. (2021, March 4). Thousands of Android and iOS Apps Leak Data From the Cloud. Wired. https://www.wired.com/story/ios-android-leaky-apps-cloud/
44, 49, 53. Google Project Zero. (2021). 0day "In the Wild." Google Docs. https://docs.google.com/spreadsheets/u/1/d/1IkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit#gid=2129022708
45. Stone, M. (2021, July 14). How we protect users from 0-day attacks. Google. https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
46. Zerodium. (2021). How to Sell Your Zero-Day (0day) Exploit. http://zerodium.com/program.html
47. CVE Details. (2021). Google Android : CVE security vulnerabilities, versions and detailed reports. https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
48. CVE Details. (2021). Apple iPhone OS : CVE security vulnerabilities, versions and detailed reports. https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49
50. Verizon. (2021). 2021 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
51. Johnson, J. (2021, September 9). Phishing - statistics & facts. Statista. https://www.statista.com/topics/8385/phishing/
52. Apple. (2021) Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading October 2021. https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf
54. L. Ceci. (2021). Mobile app usage - Statistics & Facts. Statista. https://www.statista.com/topics/1002/mobile-app-usage/
55, 56, 57. Zimperium. (2021) - When did your organization actively enable BYOD?. Pulse QA
58. Woollacott, E. (2021, January 4). Fines against banks for data breaches and noncompliance more than doubled in 2020. The Daily Swig | Cybersecurity News and Views. https://portswigger.net/daily-swig/fines-against-banks-for-data-breachesand-noncompliance-more-than-doubled-in-2020
59. Verizon Business. (2021). 2021 Mobile Security Index. https://www.verizon.com/business/resources/reports/mobile-security-index/
60. Humphries, M. (2022, January 28). Did You Install This Malicious Android 2FA Authenticator App? PCMAG. https://www.pcmag.com/news/did-you-install-this-malicious-android-2fa-authenticator-app
61. IDC. (2021). 2021 Smartphone Growth to Reach Its Highest Level Since 2015, According to IDC. https://www.idc.com/getdoc.jsp?containerId=prUS47770921&utm_medium=rss_feed&utm_source=alert&utm_campaign=rss_syndication
62. WikiWand. (2021). List of countries by number of mobile phones in use. https://www.wikiwand.com/en/List_of_countries_by_number_of_mobile_phones_in_use
63. NIST. (2021). Attack Surface · Mobile Threat Catalogue. https://pages.nist.gov/mobile-threat-catalogue/background/mobile-attack-surface/
64. Qualcomm. (2022). Snapdragon 8 Gen 1 Mobile Platform. https://www.qualcomm.com/products/snapdragon-8-gen-1-mobile-platform
65. Rutnik, M. (2022). When will your phone get the Android 11 update?. Android Authority. https://www.androidauthority.com/android-11-update-tracker-1155652/
66. Durand, J. (2021, October 26). The IoT is Breeding Killer Botnets. Device Authenticity and Data Integrity Can Save It | IOT. MyTechMag. https://iot.mytechmag.com/the-iot-is-breeding-killer-botnets-device-authenticity-and-data-integrity-cansave-it-1336.html
67. Zimperium. (2021)., Has your organization enabled employees to access Office 365 from mobile endpoints?. Pulse QA
68. Zimperium. (2021). What is your organization's current status for implementing endpoint security to protect O365 on mobile devices?. Pulse QA
69. NIST. (2021b). Glossary | CSRC. https://csrc.nist.gov/glossary/term/compromise
70. NIST. (2021b). Glossary | CSRC. https://csrc.nist.gov/glossary/term/malware
71. NIST. (2021b). Glossary | CSRC. https://csrc.nist.gov/glossary/term/mitm

Glossary of Terms

Known Malicious Network

locations previously detected with risky networks and attacks. Can include an open Wi-Fi network that presents persistent security risks to devices that connect to it

Device Compromise

A cybersecurity incident where unauthorized access to a device that undermines the endpoint's confidentiality, integrity, or availability. Impacted resources can include manipulation, theft, modification, substitution, or use of sensitive information[69]

Malicious Website

A compromised or malicious website that is part of a phishing or spear-phishing attack chain masquerading as a legitimate or reputable source in an attempt to steal sensitive information, execute an exploit, or sideload malicious applications

Malware

A malicious software or firmware that can be file-based or fileless malware used to perform unauthorized activities on a device to undermine an information system's confidentiality, integrity, or availability. Examples of this malicious code include a virus, worm, Trojan horse, spyware, and adware[70]

MITM

Man in the Middle

An attack that uses insecure networks to intercept and modify data during its transmission between a device and application. MitM can be used to compromise personal information, like login credentials[71]

Phishing / Smishing

A widespread social engineering attack vector using authentic-looking assets, such as e-mail, webpages, and text messages, to trick users to reveal critical data or direct them to a fake website that requests information. Spear phishing, or smishing, is a direct-target form of phishing

Rogue Access Point

A wireless access point that has been installed on a network's wired infrastructure without the consent of the network's owner. Often used for various attacks, including denial of service, data theft, and other malware deployment

Scan

Malicious actor is scanning across a network during the reconnaissance phase of an attack to find hosts, identify devices, and collect information for use in subsequent stages of an attack

Traffic Manipulation

A tactic deployed across multiple traffic-based threats, including SSL Stripping, Traffic Tampering, and TLS Downgrade. Malicious actors can use external, forced reductions to traffic security or packet manipulation

Danksagung

Mitwirkende Zimperium-Autoren
Adam Wosotowsky
Asaf Peleg
Esteban Pellegrino
Jon Paterson
JT Keating
Kern Smith
Krishna Vishnubholta
Monique Becenti
Nico Chiaraviglio
Richard Melick
Santiago Rodriguez
Shridhar Mittal
Jessica Vose

Mitwirkende Partner-Autoren
Julian Durand, VP Product Management, Intertrust
Loren Russon, Vice President of Product Management, Ping Identity
Rick Bosworth, Director of Product Marketing, SentinelOne

Besonderer Dank gilt
Malcolm Harkins
TK Kellerman

Redakteure
Eric Block
Jennifer VanAntwerp
Jessica Vose
Karen Walsh
Randy Budde
Richard Melick

Layout und Gestaltung
Tom Green

Über Zimperium/ Rechtliches

Zimperium basiert auf der Prämisse, dass mobile Sicherheit einen völlig neuen Ansatz erfordert und schützt sowohl mobile Geräte als auch Anwendungen, so dass diese gefahrlos und ohne Risiko auf Daten zugreifen können. Eine einzige einheitliche Plattform schützt das Endgerät und sichert den gesamten Anwendungsentwicklungszyklus mit der einzigen auf maschinellem Lernen basierenden Engine direkt auf dem Gerät. Zimperium bietet Transparenz und Schutz vor bekannten und Zero-Day-Bedrohungen und Angriffen über Geräte-, Netzwerk-, Phishing- und Anwendungsbedrohungsvektoren für Android-, iOS- und ChromeOS-Geräte. Zimperium hat seinen Hauptsitz in Dallas (Texas, USA) und wird von Warburg Pincus, SoftBank, Samsung, Sierra Ventures und Telstra Ventures unterstützt.

Weitere Informationen oder Kontaktdaten finden Sie unter zimperium.com.

ZIMPERIUM®

Haftungsausschluss

Zimperium, Inc. stellt diesen Bericht auf einer „wie besehen"-Basis zur Verfügung und übernimmt keine Garantie für Vollständigkeit, Genauigkeit, Nützlichkeit oder Aktualität. Die in diesem Bericht enthaltenen Informationen sind allgemeiner Natur. Die dargestellten Meinungen und Schlussfolgerungen spiegeln die Einschätzung zum Zeitpunkt der Veröffentlichung wider und können sich jederzeit ändern. Zimperium, Inc. übernimmt keine Verantwortung oder Haftung für Fehler, Auslassungen oder für die Ergebnisse, die durch die Nutzung der Informationen erzielt werden. Wenn Sie spezielle Probleme mit der Sicherheit von mobilen Endgeräten oder Anwendungen haben, wenden Sie sich bitte an Zimperium, Inc. unter https://www.zimperium.com/contact-us/.