ZIMPERIUM®

Management ist nicht Sicherheit

Warum die Abwehr mobiler Bedrohungen ein wesentlicher Bestandteil der Cybersicherheitsstrategie geworden ist

Vor einigen Jahren wäre das Abrufen von Firmen-E-Mails von einem privaten Gerät aus bei Ihrem Arbeitgeber möglicherweise verpönt gewesen. Die Nutzung persönlicher Geräte am Arbeitsplatz ist jedoch mittlerweile Standard in einer Unternehmensorganisation geworden. **Laut Zimperium's 2022 Global Mobile Threat Report sind 66 % der am Arbeitsplatz verwendeten Mobiltelefone Eigentum der Mitarbeiter.**

Die COVID-19-Pandemie und die Fernarbeit sind teilweise für diesen Wandel verantwortlich. So nutzen Mitarbeiter beispielsweise Produktivitätsanwendungen wie Office 365, G Suite, JIRA, Okta und Salesforce von ihren persönlichen Geräten aus, auch wenn sie im Büro und nicht nur von zu Hause aus arbeiten. Und sowohl persönliche als auch unternehmenseigene Geräte werden routinemäßig für die Multi-Faktor-Authentifizierung (MFA) verwendet, wodurch auch der nicht-mobile Zugriff auf Unternehmensdaten möglich wird.

Die Nutzung persönlicher Geräte am Arbeitsplatz steigert die Produktivität der Mitarbeiter. Allerdings verschwimmen dadurch auch die Grenzen zwischen Geräten und Daten, so dass Cyber-Kriminelle eine Fundgrube an Unternehmensdaten vorfinden, die sie gerne stehlen. Infolgedessen entwickeln die Angreifer ihre Taktik weiter und nutzen mehrere Kanäle, um Phishing-Angriffe auszuführen, wobei das Mobiltelefon die neue Hintertür ist.

Mobile Geräte sind direkt mit der Identität einer Person verbunden. Diese Geräte werden verwendet, um die Identität einer Person zu überprüfen, um Zugang zu Arbeitsdaten außerhalb der traditionellen Büroumgebung zu erhalten. Angreifer haben es auf die Benutzer mobiler Geräte abgesehen, da diese mehr Zugriff auf die Daten eines Unternehmens als je zuvor bieten und viel weniger geschützt sind als herkömmliche Endgeräte. **Herkömmliche Sicherheits- und Verwaltungskontrollen, wie z. B. Mobile Device Management (MDM), sind unzureichend, wenn es darum geht, fortschrittliche Bedrohungen effektiv zu erkennen und zu bekämpfen. Wie der Name schon sagt, verwalten MDMs nur ein Gerät.** Proaktivere Tools für die mobile Sicherheit, wie Mobile Threat Defense (MTD), sind notwendig, um Ihr Unternehmen sowohl vor Angreifern als auch vor Ihren Mitarbeitern selbst zu schützen.

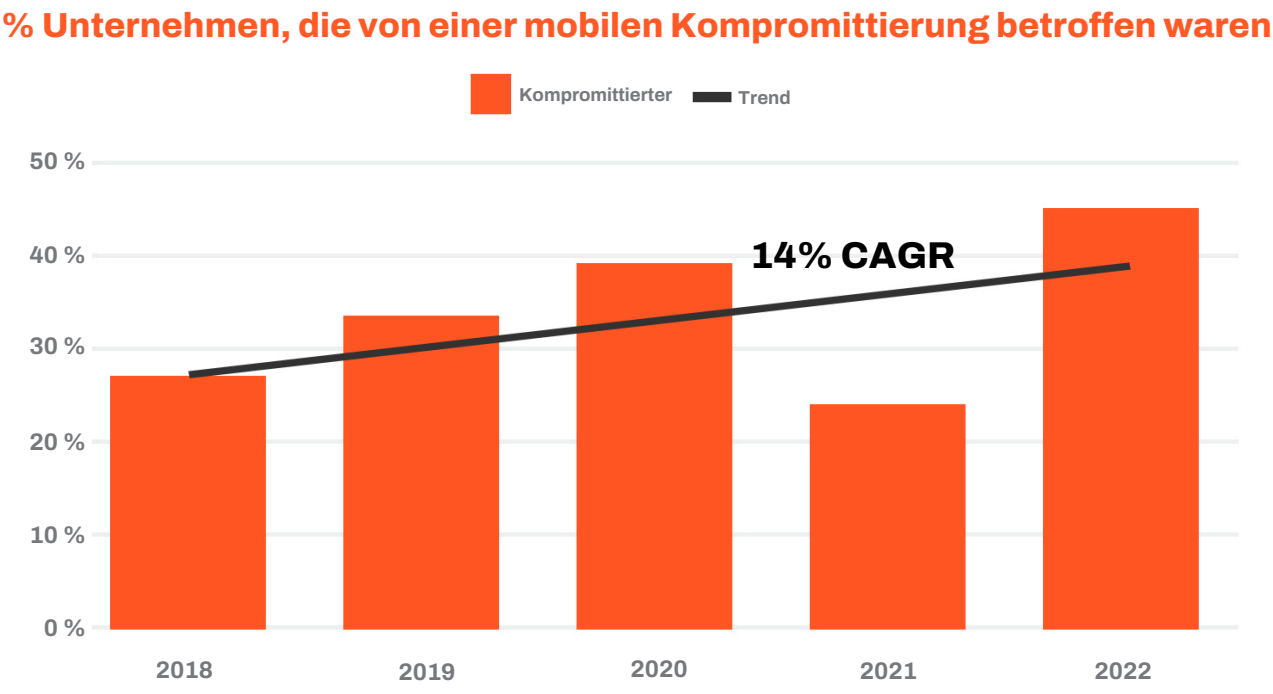


Abbildung 1. Prozentsatz der Befragten, die zugaben, dass ihr Unternehmen von einer Kompromittierung betroffen war, die ein mobiles Gerät betraf und zu Datenverlusten oder Ausfallzeiten führte.
[n=601, 671, 876, 856, 632]

(Quelle: The Verizon Mobile Security Index 2022)

Die Auswirkungen von BYOD

BYOD hat sich allein in den letzten paar Jahren dramatisch verändert. Vor der COVID-19-Pandemie, berichteten 60 % der Unternehmen, dass sie keine BYOD-Richtlinie hatten. Das hat sich zwar geändert, aber es gibt immer noch eine beträchtliche Anzahl von Unternehmen, die keine BYOD-Richtlinie haben; fast 30 %, laut unserem 2022 Global Mobile Threat Report.

Bei der Überprüfung des Bestandes an mobilen Geräten in einer Unternehmensumgebung war es überraschend, dass viele dieser Geräte, die entweder über E-Mail, Apps oder andere Kommunikationskanäle auf Unternehmensdaten zugreifen, nicht durch eine umfassende mobile Sicherheitslösung geschützt sind. Die von einem MDM verwalteten Geräte verfügen über einen Agenten, der ein mobiles Gerät kontrolliert und die Möglichkeit hat, ein mobiles Gerät zu löschen, wenn es nicht den Richtlinien entspricht, was dazu führt, dass viele Mitarbeiter nicht bereit sind, die Richtlinien für verwaltete Geräte einzuhalten. **Zimperium fand heraus, dass durchschnittlich 66 % der mit dem Unternehmen verbundenen Smartphones nicht verwaltet werden, und 5 % der Befragten sind sich nicht sicher, ob ihre Geräte überhaupt verwaltet werden.**

Ein beträchtlicher Teil des Platzes auf einem durchschnittlichen Telefon ist der Arbeit gewidmet: 10 % der auf einem mobilen Gerät installierten Anwendungen sind arbeitsbezogen. Wenn man bedenkt, dass auf einem durchschnittlichen Telefon zwischen 100 und 120 Anwendungen installiert sind, bedeutet dies, dass etwa 10 bis 12 Arbeitsanwendungen auf den Telefonen Ihrer Mitarbeiter installiert sind.

Angenommen, diese Geräte werden nicht überwacht und geschützt. In diesem Fall können vertrauliche Unternehmensdaten oder Anmeldeinformationen durch mobile Trojaner, Man-in-the-Middle (MiTM)-Netzwerkangriffe oder schlimmer noch: Ransomware, Phishing-Taktiken und sogar bösartige Apps abgefangen werden. Die meisten Benutzer wissen wahrscheinlich gar nicht, dass sie diese Bedrohungen auf ihren mobilen Geräten haben, bis es zu spät ist. Es steht viel auf dem Spiel: die durchschnittlichen Kosten einer Datenschutzverletzung betrugen im Jahr 2021 4,24 Millionen Dollar. Die Verstöße, die auf Fernarbeit zurückzuführen sind, waren sogar noch teurer, etwa 1,07 Millionen Dollar mehr.

Wie Bedrohungsakteure die erweiterte Angriffsfläche ausnutzen

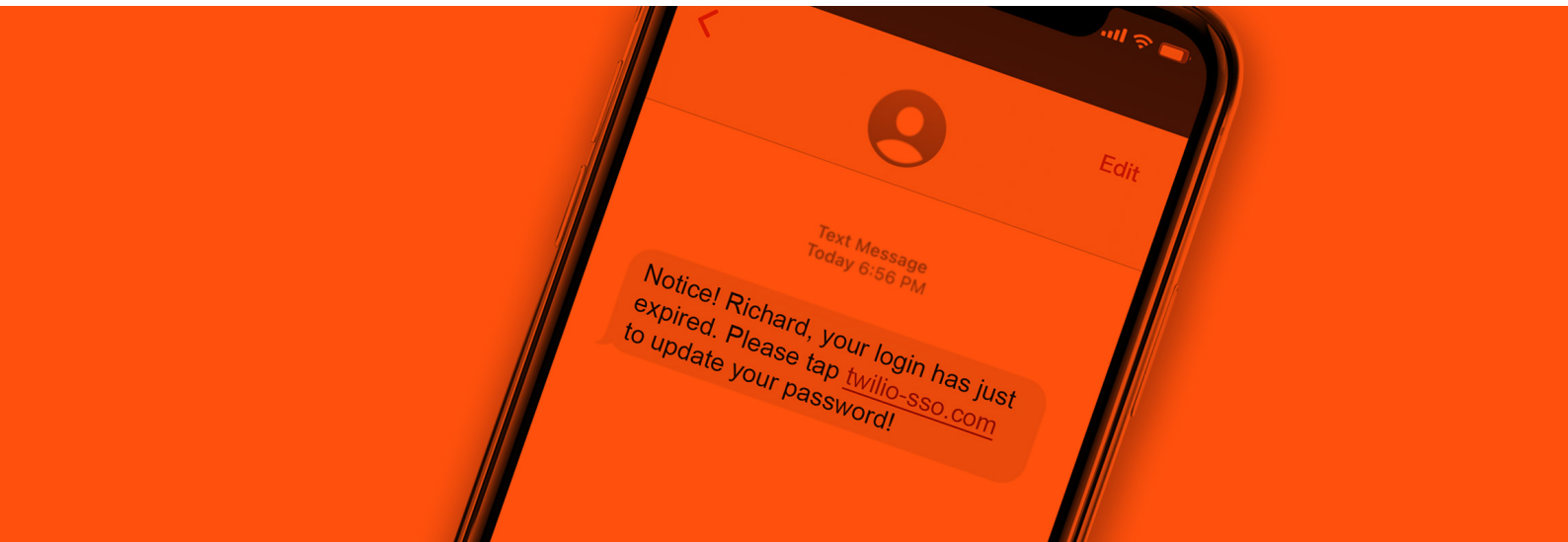
Noch vor einem Jahrzehnt mussten sich IT-Abteilungen wesentlich weniger Sorgen machen, wenn es um den Schutz ihrer Organisation vor Angriffen ging. Die Sicherheit hat sich über den „Schutz der Grenzen“ hinaus entwickelt. Herkömmliche Endgeräte, wie z. B. Desktops, befinden sich nicht mehr vor Ort und sind Eigentum des Unternehmens. In der Vergangenheit wurden diese Werte vor Ort durch verschiedene Sicherheitsebenen geschützt.

Smartphones und Tablets sind mobile Geräte, die die Art und Weise, wie wir mit Familie, Freunden und Kollegen in Verbindung bleiben, verändert haben. Mit dem Zugang der Mitarbeiter zu Kommunikationskanälen wie E-Mail, SMS, Apps und Messaging-Apps sind jedoch neue Risiken am Arbeitsplatz entstanden.

Eigene Geräte der Mitarbeiter sind schwer zu verwalten und bieten nicht die nötige Transparenz, um moderne Bedrohungen abzuwehren, selbst wenn sie unter der Unternehmensverwaltung registriert sind. Für IT-Teams ist es schwierig, Bedrohungen zu beseitigen oder risikobehaftete Geräte zu identifizieren, da sie keine angemessene Kontrolle über diese Geräte haben, weil sie nicht über die gleichen Kontrollmöglichkeiten und Berechtigungen verfügen wie der Gerätebesitzer. Firmeneigene Geräte stehen jedoch vor den gleichen Herausforderungen. Tatsächlich gaben **42 % der Unternehmen an, dass ihre mobilen Geräte und Webanwendungen im Jahr 2020 zu einem Sicherheitsvorfall geführt haben.** Derselbe Prozentsatz gab an, dass nicht autorisierte Apps am Arbeitsplatz Zugriff auf Unternehmensdaten haben und 10 % der IT- und Sicherheitsverantwortlichen berichteten über unsichere Apps aufgrund mangelnder Verschlüsselung oder Authentifizierung.

Mobile Bedrohungen sind nicht die einzigen Risiken, über die sich Unternehmen Gedanken machen sollten. Selbst Anwendungen, von denen man annehmen könnte, dass sie streng geschützt sind, fallen regelmäßig verschiedenen Arten von Malware zum Opfer. Die Apps, die Sie von einem offiziellen App-Store erhalten, sind in der Regel sicher, aber es gibt auch einige, die die Prüfung bestehen und dennoch Malware enthalten. Um nur ein Beispiel zu nennen: Laut einer Untersuchung von Zimperium sind 121 Finanz-Apps in den USA, einschließlich mobiler Geldbörsen und Banking-Apps, Ziel von Trojanern, die verschiedene Methoden nutzen, um auf sensible Daten zuzugreifen, Zugangsdaten zu stehlen und gestohlene Informationen weiterzugeben. Diese Malware ist in einer normal aussehenden App getarnt und versteckt und wird zumeist über die großen App Stores auf die Geräte heruntergeladen.

Bedrohungsakteure setzen darauf, dass viele Apps nicht abgesichert sind und die Benutzer wenig auf die Berechtigungen und Einstellungen achten, die dazu beitragen, ihre Geräte angreifbar zu machen. Infolgedessen werden mobile Geräte als die neue goldene Eintrittskarte zu Unternehmensdaten angesehen. Bösartige Anwendungen, unsichere Netzwerke oder die Kompromittierung des Geräts selbst sind nur einige der Möglichkeiten, mit denen Angreifer versuchen, Zugang zu Unternehmensressourcen zu erhalten. So hat beispielsweise das Cloud-Kommunikationsunternehmen Twilio vor kurzem eine Datenschutzverletzung bekannt gegeben, nachdem seine Mitarbeiter durch einen SMS-Speer-Phishing-Angriff betroffen waren. „Die SMS-Phishing-Nachrichten köderten die Mitarbeiter von Twilio mit der Warnung, dass ihre Passwörter abgelaufen sind oder geändert werden sollten, damit sie auf die eingebetteten Links klicken.“



Eine Einführung in Mobile Threat Defense

Da sich die Technologie weiterentwickelt, um neue geschäftliche Herausforderungen und Anforderungen zu erfüllen, hat das moderne mobile Zeitalter eine neue Sicherheitskategorie hervorgebracht, die bei der Bekämpfung aktueller Bedrohungen hilft. Mobile Threat Defense (MTD) ist eine umfassende mobile Sicherheitslösung, die mobile Bedrohungen über Geräte, Netzwerke und Anwendungen hinweg verhindert und erkennt. MTD nutzt verschiedene Techniken wie maschinelles Lernen (ML) und Verhaltensanalysen zur Erkennung von Bedrohungen, zur Überprüfung von Anwendungen und zur Verwaltung von Schwachstellen in Geräten.

Obwohl MTD und MDM ein gemeinsames Ziel verfolgen, nämlich Ihr Unternehmen vor mobilen Bedrohungen zu schützen, ist MTD eine fortschrittliche Ergänzung der Technologie für mobile Sicherheit. MTD-Tools sind im letzten Jahrzehnt auf den Markt gekommen, aber die meisten von ihnen bieten keinen umfassenden Schutz auf dem Gerät und müssen aktualisiert oder mit einem aktiven Netzwerk verbunden werden.

Die erste veröffentlichte Erwähnung der Lösungskategorie erschien als Mobile Advanced Threat Defense (MATD) in Gartners 2014 Hype Cycle for Enterprise Mobile Security. Damals wurde MATD als eine Untergruppe des ATD-Marktes (Advanced Threat Defense) betrachtet. MTD wurde jedoch bald zu einem eigenen Lösungsmarkt und erschien als MTD in einer Präsentation auf dem Gartner EMEA IT Infrastructure and Operations Management Summit in dem gleichen Jahr.

Mobile Threat Defense ist eine proaktive Methode zum Schutz mobiler Endgeräte vor Angriffen und Bedrohungen. MTD fungiert als umfassendes Alarmsystem, das ein Gerät kontinuierlich scannt, um es vor Bedrohungen zu schützen. Wenn ein Gerät nicht sicher ist, d. h. es gibt einen Angriff oder eine Schwachstelle wie z. B. nicht gepatchte Software, werden sowohl der Benutzer als auch das Unternehmen benachrichtigt.

Sichern Sie mobile Geräte oder verwalten Sie sie nur?

MDM ist, wie der Name schon sagt, ein Verwaltungstool. Ein MDM steuert das Gerät selbst und ermöglicht Unternehmen die sichere Verteilung von Apps, die Festlegung von Mindestanforderungen an das Betriebssystem (OS) und das Sperren von Apps.

MDMs bieten einen grundlegenden Schutz vor Bedrohungen, indem sie Sicherheitsteams benachrichtigen, wenn jemand versucht, das Gerät zu manipulieren. Wenn Sie Ihr Unternehmen jedoch vor möglichst vielen der im MITRE ATT&CK-Framework genannten Bedrohungen schützen möchten, müssten Sie die Nutzung des Geräts allein durch MDM in einem nahezu unmöglichen Ausmaß einschränken. Außerdem würden Ihre Benutzer die Kontrolle wahrscheinlich ablehnen und sich Sorgen um die Privatsphäre ihrer persönlichen Geräte, Anwendungen und Daten machen. Außerdem wären Sie nicht in der Lage, Bedrohungen durch Netzwerke, Phishing oder Anwendungen zu erkennen oder zu beseitigen.

MTD prüft auf verschiedene Arten von Angriffen, wie SSL-Stripping, Man in the Middle (MiTM), Phishing, Betrügerische Netzwerke, Malware und andere Angriffe. Eine umfassende Lösung wird auf dem Gerät und durch maschinelles Lernen eingesetzt, um mobile Bedrohungen über Geräte, Netzwerke, Phishing und Angriffe mit bösartigen Apps zu erkennen und zu verhindern. Mit einer MTD-Lösung hat Ihr Sicherheitsteam mehr Kontrolle über die Sicherheitsrichtlinien, die erforderlich sind, um strenge Sicherheits- und Compliance-Vorgaben zu erfüllen. Außerdem sollten MTD-Anbieter Datenschutzrichtlinien einführen, damit die Mitarbeiter besser verstehen können, wie mit den Daten umgegangen wird, ohne ihre Privatsphäre zu gefährden, während ihre Geräte geschützt werden.

Die gemeinsame Nutzung von MTD- und MDM-Tools bringt einige Vorteile mit sich. Sobald beispielsweise ein MDM ein mobiles Gerät registriert hat, Richtlinien angewendet und der Zugriff auf Unternehmensressourcen gewährt wurde, haben die Mitarbeiter nur noch begrenzte Einschränkungen, die sie in ihrer täglichen Produktivität beeinträchtigen. Die Sicherheitsteams können die Geräte in Echtzeit überwachen und die MTD-App sicher auf das Gerät übertragen, ohne dass ein kleiner oder gar kein Installationsschritt erforderlich ist, was die Akzeptanzrate eines Unternehmens deutlich erhöht und gleichzeitig die Privatsphäre der Mitarbeiter schützt.

Sicherheit mobiler Daten und Bedenken hinsichtlich des Datenschutzes

Mehr als die Hälfte (60 %) der Unternehmen erlauben ihren Mitarbeitern den E-Mail-Zugriff über ihre mobilen Geräte, weitere 31 % ziehen dies in Betracht. Die Sicherung von BYOD kann aus mehreren Gründen schwieriger sein als die Sicherung eines unternehmenseigenen Geräts. Zunächst einmal ist ein Gerät, das den Mitarbeitern gehört, genau das: Eigentum des Mitarbeiters. Als Arbeitnehmer empfindet man es als aufdringlich, wenn einem der Arbeitgeber sagt, was man herunterladen darf und was nicht.

Die Installation eines On-Device-Agenten zum Scannen des mobilen Ökosystems im Besitz eines Mitarbeiters kann ebenfalls als Eingriff in die Privatsphäre angesehen werden. Je nach Sicherheitsanforderungen können Unternehmen, die ein MDM nutzen, E-Mail-Konten einrichten, Apps aus einem App Store herunterladen und einschränken sowie persönliche Daten und Zahlungsinformationen heimlich erfassen, um sicherzustellen, dass das Gerät des Mitarbeiters den Vorschriften entspricht. Natürlich werden die Mitarbeiter Bedenken haben, wie ihre Daten und ihr Standort vom Sicherheitsteam behandelt werden.

Aus diesen Gründen ist die Akzeptanz von Sicherheitsteams bei der Absicherung von BYOD sehr gering. Die Mitarbeiter wollen wissen, dass ihre Privatsphäre respektiert wird und dass aus Sicherheitsgründen nur eine angemessene Menge und Qualität von Daten von ihrem Gerät erfasst wird.

Bei der Wahrung der Privatsphäre der Mitarbeiter ist es von entscheidender Bedeutung, dass die Vertraulichkeit der persönlichen Daten eines Nutzers geschützt wird. Die Einhaltung der geltenden Datenschutzgesetze und -vorschriften ist ein guter Anfang, um sicherzustellen, dass die Daten den Compliance-Standards entsprechen. Sicherheitsteams, die mobile Sicherheit implementieren, sollten sich mit ihren Anwälten beraten, um festzustellen, welche Datenschutzgesetze und -vorschriften sie je nach Standort und Branche einhalten müssen. Die Integration dieser Anforderungen in Ihre mobile Sicherheitsarchitektur mit Datenschutzrichtlinien, Datenschutzempfehlungen und auffälligen Datenschutzbenachrichtigungen auf den Geräten der Mitarbeiter trägt dazu bei, diese darüber aufzuklären, warum die Sicherung ihrer Geräte wichtig ist, um ihre persönlichen Daten zu schützen.

Häufige mobile Bedrohungen

Kriminelle gehen immer dorthin, wo das Geld ist. Früher haben sie Postkutschen und Banken ausgeraubt. Die Daten Ihres Unternehmens sind jetzt bares Geld wert und da immer mehr Mitarbeiter ihre privaten Mobilgeräte am Arbeitsplatz nutzen, haben es Kriminelle auf diese mobilen Endgeräte abgesehen. Hier sind einige der häufigsten mobilen Bedrohungen, die unser Team beobachtet:

Phishing

Phishing ist eine allgegenwärtige Cyber-Bedrohung, wahrscheinlich weil Cyber-Kriminelle wissen, dass es funktioniert. Trotz der Tatsache, dass die Benutzer oft geschult sind, Phishing-Betrügereien zu erkennen und zu vermeiden, ergab die Untersuchung von Zimperium, dass im Jahr 2021 einer von zehn mobilen Benutzern auf einen bösartigen Link geklickt hat. Tatsächlich beginnen 90 % der Angriffe mit einer Phishing-Attacke und Ihre Benutzer rufen ihre Arbeits-E-Mails wahrscheinlich über ihr Telefon ab.

Malware

Herr Malware ist eine häufige Bedrohung, die mobile Geräte in einem ernüchternden Ausmaß betrifft. Jedes vierte mobile Endgerät war 2021 mit Malware konfrontiert und laut einer aktuellen Umfrage unter IT- und Sicherheitsverantwortlichen hatten 52 % der Unternehmen mit Malware-Angriffen zu kämpfen, darunter Viren und Ransomware. Trojaner sind ein Beispiel für mobile Malware, die in mobilen Anwendungen zu finden ist, die Benutzer unwissentlich herunterladen.

Null-Klick-Angriffe

Null-Klick-Angriffe sind Angriffe, bei denen der Benutzer den Angriff nicht durch Klicken auf einen bösartigen Link auslöst. Bei einem Null-Klick-Angriff ist der Angreifer in der Lage, zuvor unbekannte Schwachstellen auszunutzen, um einen eigenen Einstiegspunkt in das Gerät zu schaffen. Die Ausnutzung von Null-Klick-Schwachstellen in mobilen Geräten nimmt zu. Im Jahr 2021 stiegen solche Angriffe sowohl bei Android- als auch bei iOS-Geräten um 466 %.

Betrügerische WLAN-Netzwerke

Mobile Geräte stellen eine Verbindung zu einem beliebigen WLAN-Netzwerk her, wenn der Mobilfunkdienst schwach ist, was sie zu leichten Zielen für Angreifer macht. WLAN-Netzwerke können von böswilligen Akteuren leicht ausgenutzt werden. Betrügerische WLAN-Netzwerke sind eine der besten Möglichkeiten für Kriminelle, ein Gerät zu kompromittieren. Ein Angreifer kann ein gefälschtes WLAN-Netzwerk mit einem gewöhnlichen Namen wie „Coffee Shop Guest“ verwenden und sich so sofort Ihr Vertrauen erschleichen. Dieses betrügerische Netzwerk dient jedoch als Einfallstor für einen Man-in-the-Middle-Angriff, um Ihre Aktivitäten auszuspionieren, Informationen zu stehlen oder Malware zu starten, um Anmeldedaten zu stehlen.

Mobil-spezifische Sicherheitsüberlegungen

Es ist wichtig zu verstehen, dass die mobile Sicherheit andere Maßnahmen erfordert als die traditionelle Cybersicherheit. Die Technologie eines mobilen Geräts funktioniert anders als die eines herkömmlichen Endgerätes und daher müssen andere Sicherheitsaspekte berücksichtigt werden. Hier sind zwei der am häufigsten zitierten mobil-spezifischen Überlegungen:

Gerätestatus

Der Gerätestatus ist ein Indikator dafür, ob Software frei auf ein Gerät übertragen werden kann und ob eine Verifizierung erzwungen wird. Bei Android gibt es zwei Status: Gesperrt und Entsperrt. iOS-Geräte hingegen dürfen nur gesperrt werden, obwohl sie manipuliert werden können, um einem Benutzer Root-Zugriff zu gewähren und Apples Einschränkungen zu umgehen.

Ein entsperrtes Android-Gerät birgt jedoch Sicherheitsrisiken. Wenn ein Android-Gerät entsperrt ist, kann ein bösartiger Akteur, der die physische Kontrolle über das Gerät erlangt, das Gerät neu starten und auf die Daten zugreifen, wobei er die Sicherheitsmaßnahmen umgeht, die ihn davon abhalten sollen. Gleichermaßen ist ein manipuliertes iPhone anfälliger für Malware und andere Bedrohungen.

Anfällige Anwendungen

Mobile Anwendungen sind eine Quelle der Unterhaltung auf unseren mobilen Geräten, die Produktivität am Arbeitsplatz ermöglichen und unsere Finanzen mit Banking-Apps in Ordnung halten. Heutzutage sind 120 Apps auf einem Smartphone gespeichert. Schwachstellen in Anwendungen sind jedoch häufiger, als Sie vielleicht denken. Der Code von Entwicklern mobiler Anwendungen kann Mitarbeiter- und Kundendaten preisgeben und so den Datenschutz und die Sicherheit gefährden. Mobile Apps können von Angreifern heruntergeladen und zurückentwickelt oder so umgebaut werden, dass sie eine gängige Marke imitieren, mit der Absicht, vertrauliche Berechtigungen auf einem Gerät zu aktivieren und so jedes Passwort und jede SMS-Nachricht an einen Angreifer weiterzugeben.

Die Rolle des maschinellen Lernens bei der Erkennung von Bedrohungen

Der proaktive Ansatz von MTD wird durch maschinelles Lernen (ML) ermöglicht, eine Art von künstlicher Intelligenz, die Algorithmen verwendet, um immer genauere Vorhersagen zu treffen, wenn ein ML-Modell mehr und mehr Informationen sammelt.

Ein Modell für maschinelles Lernen wird durch Training und Abstimmung erstellt. Ein Algorithmus wird einem Satz von Trainingsdaten ausgesetzt. Anhand der Trainingsdaten lernt das Modell, wonach es in Datensätzen (wie Bedrohungsdaten) suchen soll. Nach dem anfänglichen Training wird das Modell mit Daten konfrontiert, die es noch nie zuvor gesehen hat, um zu sehen, ob es die richtigen Schlüsse zieht. Datenwissenschaftler stimmen das Modell dann ab, indem sie es immer mehr Daten aussetzen und ihm helfen zu lernen.

Wie sieht das bei der Erkennung von Bedrohungen aus? ML-Modelle verwenden verschiedene Methoden, um Angriffe zu erkennen. So kann ein Klassifikator beispielsweise die Wahrscheinlichkeit bestimmen, dass ein Link Teil eines Phishing-Betrugs ist oder dass es sich bei einer App tatsächlich um Malware handelt.

Um eine möglichst unmittelbare Erkennung von Bedrohungen zu erreichen, muss maschinelles Lernen auf dem Gerät selbst und nicht in der Cloud eingesetzt werden, damit das Gerät auch dann geschützt ist, wenn es nicht mit einem Netzwerk verbunden ist. Ein Sicherheitsverstoß kann schnell passieren, innerhalb von Millisekunden. Die Algorithmen für das maschinelle Lernen müssen lokal sein, damit sie so schnell wie möglich reagieren können und nicht von einem schwachen WLAN oder Mobilfunkdiensten abhängig sind.

Top-Empfehlungen für die Implementierung von MTD

Bei der Implementierung einer MTD-Lösung haben Unternehmen verschiedene Möglichkeiten. Ein MTD kann für sich alleine stehen oder zusammen mit anderen Unified Endpoint Management (UEM)-Lösungen oder MDM verwendet werden.

In Verbindung mit einer MDM-Lösung fungiert MTD als integrierter Bestandteil der Sicherheitsstrategie für mobile Endgeräte und schützt das Gerät selbst vor mobilen Bedrohungen, anstatt das Gerät zu verwalten. **Die MDM-Verwaltungsrichtlinien ermöglichen die Automatisierung, wie z. B. den Download der MTD-App und die Aktivierung von MTD-Erkennungen, und erleichtern dem Administrator die Automatisierung von bedingtem Zugriff und Sicherheitsrichtlinien auf der Grundlage von Erkennungen und Richtlinien der MTD-Lösung.**

Wenn sich ein Benutzer beispielsweise in einem betrügerischen WLAN-Netzwerk befindet, warnt ein MTD den Benutzer und das Unternehmen vor der Bedrohung und arbeitet mit Ihrem MDM zusammen, um den Zugriff auf geschäftskritische Anwendungen zu sperren, bis sich der Benutzer in einem sicheren Netzwerk befindet.

In Fällen, in denen MTD allein auf einem nicht verwalteten Gerät eingesetzt wird, ist die MTD-Lösung dennoch in der Lage, viele Angriffe auf mobile Geräte zu erkennen und zu verhindern, indem sie mithilfe von maschinellem Lernen das Gerät selbst proaktiv auf schädliches Verhalten, Malware oder andere Bedrohungen untersucht. MTD benachrichtigt dann den Benutzer, kann aber nur begrenzt kontrollierte Abhilfemaßnahmen ergreifen, wie z. B. die Sperrung des Zugangs ohne die Hilfe einer integrierten UEM-Lösung.

In beiden Fällen wird die Bedrohung zwar lokal behandelt, aber das MTD meldet auch an das Unternehmen zurück, so dass das Sicherheitsteam alle aufgetretenen Bedrohungen nachvollziehen kann. Es wird jedoch dringend empfohlen, eine MTD-Lösung durch ein MDM zu ergänzen, um die Reibungsverluste für die Benutzer erheblich zu verringern. Wenn Sie beides haben, können Sie die Privatsphäre der Benutzer wahren und wichtige Geschäftsdaten schützen.

Schlussfolgerung/Empfehlungen

Nach Angaben von Verizon, auf die Frage, wie wichtig mobile Geräte auf einer Zehn-Punkte-Skala für den reibungslosen Ablauf in ihrem Unternehmen sind, antworteten 91 % der Befragten mit sieben oder mehr und 78 % mit acht oder mehr. Der Mobile Security Index 2022 erklärt, dass mobile Geräte für die Arbeitsweise von Unternehmen entscheidend sind.

Im Zusammenhang mit der mobilen Sicherheit bedeutet „blockieren und bekämpfen“, proaktiv Bedrohungen für mobile Geräte zu finden und zu beseitigen. Wenn Sie auf die Benachrichtigung über eine Sicherheitsverletzung warten, ist es bereits zu spät. Deshalb ist es wichtig, eine Bedrohung so schnell wie möglich zu erkennen.

Welche Schritte kann Ihr Unternehmen also unternehmen, um proaktiv gegen mobile Risiken vorzugehen?

1. **Analysieren Sie mobile Risiken:** Bewerten und priorisieren Sie Ihre Risiken auf der Grundlage der spezifischen Sicherheitsanforderungen Ihres Unternehmens. Wie groß ist zum Beispiel das Risiko eines gestohlenen Geräts? Was ist mit Malware oder dem persönlichen Verhalten eines Benutzers mit seinem Gerät? Durch die Erstellung eines Risikoregisters können Sie Risiken für Ihr Unternehmen schnell erkennen.

2. **Zero Trust anwenden:** Vorbei sind die Zeiten, in denen es hieß: Vertrauen, aber überprüfen. Jetzt, wo Anwendungen in der Cloud laufen und mobile Geräte am Arbeitsplatz immer wichtiger werden, ist Zero Trust für jede Sicherheitsstrategie entscheidend. Wenden Sie das Prinzip der geringsten Privilegien an, um die Sicherheit Ihrer Daten und Ihres Netzwerks zu gewährleisten.

3. **Investieren Sie in MTD:** MTD ermöglicht es Ihrem Unternehmen, Risiken zu beseitigen, sobald sie auftreten, ohne die Benutzerfreundlichkeit für Ihre Mitarbeiter zu beeinträchtigen. Laut Gartner kann MTD „für sich alleine stehen, um Zero-Trust-Zugang zu bieten, Single-Sign-On über Anwendungen hinweg zu verbinden und weiterhin Telemetrie zu generieren“, um Unternehmen dabei zu helfen, bessere, intelligentere und schnellere Zugangsentscheidungen zu treffen.

Kontaktieren Sie uns, um mehr darüber zu erfahren, wie die MTD-Lösungen von Zimperium Ihr Unternehmen proaktiv vor der sich entwickelnden Bedrohungslandschaft schützen können.

Empfohlene Lektüre

2022 Global Mobile Threat Report
Mobile Banking Heists: Die globale wirtschaftliche Bedrohung
Wie man BYOD in einer Zero-Trust-Umgebung implementiert
Der MSI Mobile Security Index 2022 von Verizon

ZIMPERIUM®

Erfahren Sie mehr unter: zimperium.com
Kontaktieren Sie uns unter: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244